Ausgabe 03/2019

ISSN: 2194-1025

BvD-NEWS

Das Fachmagazin für den Datenschutz

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Hand in Hand:

Datenschutzbeauftragte und Aufsichtsbehörden im Dialog

AUFSICHT TRIFFT WIRTSCHAFT – KONSENS ODER KONFLIKT? – S. 7

LÖSCHREGELN FÜR ISSUE-TRACKINGSYSTEME ENTWICKELN – S. 25

WEBSEITEN NACH DER DSGVO – S. 49

DATEV-STIFTUNG ZUKUNFT IST WIEDER BEI DER DAME DABEI – S. 52

BvD e.V.

DATENSCHUTZ GESTALTEN

Jetzt anmelden unter:
https://www.bvdnet.de/termine/

BvD e.V.
DATENSCHUTZ GESTALTEN

2020 BvD-Veranstaltungen

BvD-Verbandstage „Datenschutz: Made in Europe" – ein globaler Standard?

SONDERSEMINARE AM VORTAG

06.05. – 07.05.2020

ELLINGTON HOTEL BERLIN

Verleihung Datenschutz Medienpreis des BvD (DAME)

am 06.05.2020 zur Abendveranstaltung

DAME 2019 BVD DATENSCHUTZ MEDIENPREIS

BvD-Herbstkonferenz zum Datenschutz & Behördentag 2019

WIRTSCHAFT TRIFFT AUFSICHT

21.10. – 23.10.2020

STEIGENBERGER HOTEL GRAF ZEPPELIN STUTTGART

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg, das Bayerische Landesamt für Datenschutzaufsicht und der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. laden zum Informationsaustausch ein.

Gemeinsame Veranstaltung von:

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

BayLDA

BvD e.V. DATENSCHUTZ GESTALTEN

DIGITALISIERUNG UND DATENSCHUTZ GEHÖREN UNTRENNBAR ZUSAMMEN

Deutschland bei der Digitalisierung Schlusslicht – und beim Datenschutz?

Liebe Leserinnen und Leser,

Wenn es um die Digitalisierung in Deutschland geht, reißen die negativen Nachrichten nicht ab: Die Bundesregierung ringt (seit Jahren) um eine Digitalisierungsstrategie, der Netzausbau kommt nicht voran, andere EU-Länder sind bei der Digitalisierung viel weiter, lautet die Kritik. Die Bundesregierung glaubt, das liege vor allem am Datenschutz. Hier müssten Regelungen abgebaut werden, damit Daten leichter verarbeitet werden könnten – „Bürgerrechte second" sozusagen.

Vielleicht hilft ein Blick in andere Länder, die auf dem Pfad der Digitalisierung schon viel weiter sind. Lamentiert in der EU ein anderes Land so sehr über die DSGVO? Mitnichten. Biegen sich die Amerikaner vor Schadenfreude, dass die Deutschen und Europäer sich so eine Verordnung ausgedacht haben? Nein, schon lang nicht mehr. Sie fangen sogar an sie zu kopieren!

Während Deutschland lamentiert und nicht voran kommt, nutzen die digitalen Vorreiter die Vorteile der DSGVO und die Gesetze des Marktes. Denn Datenschutz schafft Transparenz und Vertrauen. Beides sind wichtige Voraussetzungen für eine weitgreifende Digitalisierung, erst recht für den Einsatz von Künstlicher Intelligenz. Dies haben auch die Amerikaner verstanden und wollen sich diesen Marktvorteil nicht entgehen lassen. Also wird der Datenschutz dort zu einem wichtigen Markenzeichen der Digitalwirtschaft – auch wenn das nicht von heute auf morgen geht, wird uns das Tempo überraschen.

Wenn aber Politik und die Wirtschaft in Deutschland sich weiter gegenseitig die Verantwortung für die bislang verschlafene Digitalisierung zuschieben, dann haben uns die anderen nicht nur bei der Digitalisierung, sondern auch beim Datenschutz und damit beim Kundenvertrauen überholt. Dann kann es Deutschland noch als eine Art analoges Museum für Touristen aus den digitalen Ländern versuchen, und das Erlebnis von Funklöchern und Kriech-Internet, W-LAN-Abstinenz und gewaltigen Behörden mit beeindruckenden Registraturen bieten. Da können sich die Besucher mal so richtig gestrig und analog fühlen. Steht es so schlimm um Deutschland? Noch nicht, aber unsere Politik arbeitet mit Hochdruck daran. Jüngstes bitteres Beispiel: Die vorbildliche und angesichts des kleinen Budgets überaus erfolgreiche Stiftung Datenschutz erhält kein neues Budget, sie kommt im neuen Bundeshaushalt schlicht nicht vor.

Erinnern wir uns: Vor dem Wirksamwerden der DSGVO war auf den Webseiten der Bundesregierung nichts an Informationen zu erhalten, nicht für Bürger und nicht für Unternehmen. Einzig die Stiftung Datenschutz hat mit viel Einsatz ihrer überaus engagierten und kompetenten Mitarbeiter herausragende Unterlagen und Informationsangebote geschaffen, die zur Vorbereitung und Information sehr gut geeignet sind und vielen geholfen haben sich auf das neue Datenschutzrecht vorzubereiten. Diese erfolgreiche Arbeit wird nun torpediert und gefährdet. Deutschland möchte beim Datenschutz kein Vorbild mehr sein. Ob das die Digitalisierung voranbringt?

Der BvD hat längst Vorschläge für Verbesserungen im Datenschutzrecht gemacht und wird mit den Kollegen aus den anderen EU-Staaten in der EFDPO, dem neuen EU-Dachverband der Datenschutzbeauftragten, weitere Vorschläge entwickeln und der EU-Kommission vorlegen.

Die BvD-Herbsttagung 2019 hat wieder sehr schön gezeigt, was alles möglich ist, wenn Datenschützer aus Aufsicht und Wirtschaft zusammen diskutieren und nach Lösungen suchen. Rund 300 Teilnehmer, Gäste und Referenten haben in Nürnberg eine spannende Veranstaltung und viele intensive Fachgespräche erlebt. Die vorliegende Ausgabe der BvD-News greift noch einmal viele der Themen aus Nürnberg auf und gibt einen Einblick in den Diskussionsstand.

Ich wünsche Ihnen eine anregende Lektüre

Ihr Thomas Spaeing
BvD-Vorstandsvorsitzende

IMPRESSUM:
BvD-News
Das Fachmagazin des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Herausgeber:
Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.
Budapester Straße 31
10787 Berlin
Tel: 030 26 36 77 60
Fax: 030 26 36 77 63
E-Mail: bvd-gs@bvdnet.de
Internet: www.bvdnet.de
www.xing.com/companies/berufsverbandderdatenschutzbeauftragtendeutschlands
www.twitter.com/bvd_datenschutz
https://www.bvdnet.de/feed/

Redaktion:
Christina Denz
V.i.S.d.P.: Thomas Spaeing
bvd-news@bvdnet.de

Fotos:
123rf.com
Shutterstock.com

Lektorat:
Frank Spaeing, Regina Mühlich

Anzeigen:
Christina Denz, Claudia Seilert
(bvd-gs@bvdnet.de)

Satz, Layout & Produktion:
Trend Point Marketing GmbH,
Breitenbachstraße 24-29, 13509 Berlin
www.tpmarketing.de

ISSN: 2194-1025
Erscheinungsweise: 3 × jährlich, ca. 4.000 Exemplare
(Unsere Mediadaten erhalten Sie unter bvd-gs@bvdnet.de)
Die Redaktion behält sich vor, Beiträge redaktionell zu überarbeiten und zu kürzen. Namentlich gekennzeichnete Beiträge müssen nicht die Meinung des BvD e.V. wiedergeben.

EDITORIAL

Digitalisierung und Datenschutz gehören untrennbar zusammen. Deutschland bei der Digitalisierung Schlusslicht – und beim Datenschutz? – *Thomas Spaeing* 3

WIRTSCHAFT UND BEHÖRDEN TREFFEN AUFSICHT

Beratung ist besser als Geldbuße – *Christina Denz* 5
Aufsicht trifft Wirtschaft – Konsens oder Konflikt? – *Dr. Stefan Brink* 7
Die Datenschutzbeauftragten, die Datenschutz-Grundverordnung und der BvD – *Prof. Dr. Thomas Petri* 11

DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)

Bußgeldbemessung: So gehen die Aufsichtsbehörden künftig vor – *Jens Eckhardt* 14
Datenschutzvorfälle – Ein Erfahrungsbericht nach eineinhalb Jahren DSGVO – *Thomas Kahl* 17
Recruiting unter der DSGVO – *Nina Diercks* 21

DATENSCHUTZPRAXIS

Löschregeln für Issue-Tracking-Systeme entwickeln – *Annika Selzer, Sarah Stummer* 25
Unterauftragsverarbeiter wechseln? – *Dr. Niels Lepperhoff* 31
Überarbeitete Praxishilfe zur DSFA im Gesundheitswesen liegt vor – *Dr. Bernd Schütze* 34

GESETZESÄNDERUNGEN

Das zweite DSAnpUG-EU und die Änderungen des BDSG – *Tilmann Dralle* 38
Der Erlaubnistatbestand des § 26 BDSG – *Heiko Schöning, LL.M.* 42

AUFSICHTSBEHÖRDEN

Scoring – Voraussetzungen und Betroffenenrechte nach der DSGVO und dem BDSG – *Daniel Joos* 45

GESELLSCHAFT

Webseiten nach der DSGVO: Längere Datenschutzerklärungen und mehr Cookie-Hinweise. – *Martin Degeling und Christine Utz* 49
Schutz von hochsensiblen Daten: Schreddern ist nicht gleich schreddern 52

AUS DEM VERBAND

Interview mit Dr. Sebastian Sprenger: DATEV-Stiftung Zukunft ist wieder bei der DAME dabei – Katrin Eggert 54
Von guter Laune und Leckerbissen – Herbstkonferenz und Behördentag in Nürnberg – *Christina Denz* 56
Jubiläum auf dem Dozententreffen von DSgzS – *Rudi Kramer* 60

REZENSIONEN

Daten- und Persönlichkeitsschutz im Arbeitsverhältnis – *Stephan Weth, Maximilian Herberger, Michael Wächter, Christoph Sorge* 62
DSGVO-Kompendium – *Dr. Jens Eckhardt, Rudi Kramer, Sebastian Tausch* 63
Mein Recht auf Datenschutz nach der Datenschutz-Grundverordnung – *Thomas Kranig, Eugen Ehmann* 64
Compliance-Nachweis zum Web-Tracking nach DSGVO – *Kristin Benedikt, Alexander Buckel, Jan-Hendrik Mammen* 65
Datenschutz-Compliance nach der DSGVO – *Thomas Kranig, Andreas Sachs, Markus Gierschmann* 66
Handbuch IT- und Datenschutzrecht – *Astrid Auer-Reinsdorff, Isabell Conrad et. al.* 67
Web-Tracking nach DSGVO – *Kristin Benedikt, Alexander Buckel, Jan-Hendrik Mammen* 68
Handbuch Beschäftigtendatenschutz – aktuelle Rechtslage und Umsetzungshilfen – *Prof. Dr. Peter Gola* 69

TERMINE UND KONTAKTE

Termine der Regionalgruppen und Arbeitskreise des BvD 70
Überblick Seminare und Workshops 2020 71

„BERATUNG IST BESSER ALS GELDBUßE“

Aufsichtsbehörden und BvD luden gemeinsam zur dritten Herbstkonferenz

Christina Denz

Der Saal ist voll, die Erwartungen groß: Knapp 300 Datenschutzbeauftragte trafen sich am 23. und 24. Oktober zur dritten BvD-Herbstkonferenz „Wirtschaft trifft Aufsicht“, zu der der BvD mit den Landesdatenschutzbeauftragten aus Bayern und Baden-Württemberg in Nürnberg geladen hatte. Eine neue Bestmarke. Den Behördentag am 25. Oktober besuchten fast 200 Datenschutzbeauftragte von Schulen, Theatern, Bibliotheken, Bürgerämtern und Verwaltungen.

Im Fokus der Vorträge und Gespräche stand erneut die DSGVO. Auf den Tag 17 Monate war sie in Nürnberg alt geworden, im Mai 2020 will die EU-Kommission ihre Evaluierung vorlegen. Von Juli bis Dezember 2020 übernimmt Deutschland die EU-Ratspräsidentschaft – und wird sich dabei auch mit den Schlussfolgerungen aus der Evaluierung befassen.

> *Der Austausch mit den Datenschutzbeauftragten auf der Herbstkonferenz ist einfach toll. Die Tagung zeigt, dass beide Seiten am Ende doch an einem Strang ziehen. Wir wollen Datenschutz zu seinem Recht verhelfen, in den Bundesländern, in Deutschland und in Europa.*
>
> ***Thomas Kranig**, Präsident Bayerisches Landesamt für Datenschutzaufsicht*

Gegen eine erneute Aufweichung der Benennungspflicht

Dafür laufen sich die Akteure bereits warm. Erst kürzlich hatte Bundeswirtschaftsminister Peter Altmaier (CDU) eine erneute Aufweichung der Benennungspflicht für Datenschutzbeauftragte ins Spiel gebracht. Der bayerische Staatsminister Joachim Herrmann (CSU) mahnte in seiner Eröffnungsrede zum Behördentag einen weiteren Bürokratieabbau an, er sprach von unternehmerischer Freiheit und dass nicht „alle Player über einen Kamm“ geschoren werden dürften. Zwar bezeichnete er die Lockerung der Benennungspflicht auf nunmehr 20 Mitarbeiter als „tragfähigen Kompromiss“. Er wolle aber die Beratungen zur Evaluierung nutzen, weitere Erleichterungen vor allem für Vereine und mittelständische Betriebe durchzusetzen.

Prof. Dr. Thomas Petri, Landesbeauftragter für den Datenschutz in Bayern und damit zuständig für den Datenschutz in öffentlichen Einrichtungen, verwies in seiner Anschlussansprache darauf, dass immer wieder das Argument des Bürokratieabbaus herangezogen würde, um die Wirtschaft von der Benennung eines Datenschutzbeauftragten zu befreien. Der behördliche Datenschutzbeauftragte, der ein originärer Bestandteil der Verwaltung sei, stehe jedoch nicht zur Debatte.

» Seinen Beitrag lesen Sie im Anschluss.

Die Aufsichtsbehörden wissen durchaus, was sie an den Datenschutzbeauftragten haben. Für einen reibungslosen Ablauf sei der Datenschutzbeauftragte „extrem wichtig“, sagte der Präsident des Bayerischen Landesamts für Datenschutzaufsicht, Thomas Kranig, der für Datenschutz in der Privatwirtschaft im Freistaat zuständig ist, in Nürnberg.

Beratung womöglich bald nicht mehr kostenlos

Kranigs Haus prüft gerade, ob sie Beratung, die sie der Wirtschaft anbietet, kostenpflichtig für jene Unternehmen macht, die keinen Datenschutzbeauftragten ernannt haben.

„Wir können die Arbeit von Datenschutzbeauftragten nicht ersetzen und Firmen beim Aufbau ihres Datenschutz-Verfahrens begleiten“, sagte Kranig. Ohnehin können die Aufsichtsbehörden ihm zufolge nur in dem Rahmen beraten, den die DSGVO dafür einräumt. Verarbeitungskonzepte durchsehen, Datenschutzbestimmungen prüfen ▸

Thomas Kranig
auf der BvD-Herbstkonferenz 2019 in Nürnberg
Foto: BvD e.V / Uli Schneider

oder Hilfe bei Verträgen mit Auftragsdatenverarbeitern seien tabu. „Wir zertifizieren nicht und vergeben keine Prüfsiegel", sagte er. Aber es gibt auch Argumente gegen eine Beratung durch die Aufsichtsbehörden, unter anderem, dass die Mitarbeiter für spätere Kontrollen befangen sein könnten. Auch dürfe keine unzulässige Konkurrenz zu freien Beratern entstehen. Zudem ist die Beratung in der DSGVO für die Aufsichtsbehörden keine Pflicht. Damit könnten Aufsichtsbehörden anderer EU-Länder darauf verzichten – was für EU-Unternehmen zu einem Ungleichgewicht führen würde.

Kranig will trotzdem die Wirtschaft beim Datenschutz unterstützen. „Beratung ist besser als Geldbuße" sagte er. Durch den Kontakt mit den Unternehmen lernten sie selbst dazu, erführen, welche Fragen immer wieder auftauchten. „Wir beraten nach pflichtgemäßem Ermessen", sagte Kranig und das heißt: In gebotener Kürze, in angemessener Zeit „und am liebsten online".

> *Auch für uns Aufsichtsbehörden ist der Austausch mit den Datenschutzbeauftragten auf der Konferenz wichtig. Ich nehme persönlich viel mit, etwa, welche Fragen die Datenschutzbeauftragten umtreiben, ob sie nun bereits viel Erfahrung haben oder noch am Anfang stehen. Und ich habe einige Visitenkarten in der Tasche, um über die Konferenz hinaus Fragen und Aspekte des Datenschutzes zu besprechen.*
>
> ***Helga Block**, Datenschutzbeauftragte des Landes Nordrhein-Westfalen*

Weiterlesen

Mehr über die Herbsttagung mit Fotos und Eindrücken der Teilnehmenden lesen Sie in der Rubrik „Aus dem Verband"

Über die Autorin

Christina Denz
ist Journalistin, Kommunikationsberaterin und Redakteurin der „BvD-News

AUFSICHT TRIFFT WIRTSCHAFT – KONSENS ODER KONFLIKT?

Dr. Stefan Brink

Zum dritten Male trafen sich im Rahmen der BvD-Herbstkonferenz, welche der Landesbeauftragte für den Datenschutz Baden-Württemberg seit 2017 mit veranstaltet, Datenschützer aus den Aufsichtsbehörden – in diesem Jahr gemeinsam mit den Kollegen – mit Berufsvertretern aus Wirtschaftsunternehmen und Behörden.

Diesen unmittelbaren Austausch sehen wir als zentrale Aufgabe an: Nur wenn wir verantwortlich miteinander sprechen, können wir uns gegenseitig optimal informieren und gleichzeitig ein Vertrauensverhältnis aufbauen, auf das wir uns bei der Klärung der zahlreichen datenschutzrechtlichen Fragen stützen können.

Was hat sich auf Seiten der Aufsichtsbehörden seit unserer letzten Konferenz getan? Schon 2018, im Jahr des Wirksamwerdens der DSGVO haben wir beraten, beraten, beraten. Das hat sich ausgezahlt. Im Jahr 2019 haben wir die Ergebnisse unserer Beratungstätigkeit durch verstärkte Kontrollen überprüft, deren Ergebnisse wir am Jahresende vorstellen werden. Ein erstes Ergebnis sei schon verraten: An Bußgeldern haben wir 2019 nicht so viele verteilt wie befürchtet. Das zeigt, dass verstärkte Kontrolltätigkeit der Aufsichtsbehörde nicht gleichbedeutend ist mit mehr Sanktionen.

Und selbst wenn es zu ahndungswürdigen Verstößen gegen den Datenschutz gekommen ist: Bußgelder gestalten wir immer verhältnismäßig. Wer bereit ist, in Maßnahmen zum Datenschutz zu investieren und sich im Rahmen der Aufklärung kooperativ zeigt, kann mit entsprechender Berücksichtigung bei der Bußgeld-Zumessung rechnen.

Unter ihrem Markenzeichen „Wirtschaft trifft Aufsicht“ stand auch die diesjährige Herbstkonferenz in Nürnberg, auf der meine Mitarbeitenden und ich Einblick in unsere behördlichen Arbeitsweisen und Positionen gaben. Dabei wurde auch eine Reihe von Einzelthemen vorgestellt, die meine Dienststelle im vergangenen Jahr beschäftigt haben und die den Teilnehmenden der diesjährigen Herbstkonferenz vorgestellt wurden. ▸

Beschäftigtendatenschutz

Bei der spannenden und viel diskutierten datenschutzrechtliche Frage, ob der Betriebsrat eine eigene verantwortliche Stelle im Sinne der DSGVO ist, steht es momentan gewissermaßen 2 zu 2. Bislang wurden vier Urteile zur Frage der Verantwortlichkeit des Betriebsrates gesprochen, zwei gehen von einer Verantwortlichkeit aus, zwei verneinen dieselbe.

Unsere Position, welche sich ebenfalls im 38. Tätigkeitsbericht wiederfindet, ist dabei klar: Der Betriebsrat ist regelmäßig Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO, Personalräte sind es in der Regel nicht.

Diese Position, welche auch andere Aufsichtsbehörden, etwa die Kollegen aus Hessen, unterstützen, wird also noch breit diskutiert. Nur durch eine klare Positionierung der Aufsichtsbehörden und im Anschluss auch der Gerichte kann hier letztlich Rechtsklarheit geschaffen werden.

(Pre-) Employment Screenings

„(Pre-) Employment-Screenings", teilweise auch „Background-Checks" oder „Bewerberscreenings" genannt, haben mittlerweile eine erhebliche Verbreitung gefunden. Das Interesse der Arbeitgeber besteht hier regelmäßig darin, die Angaben der Bewerber im Rekrutierungsverfahren zu überprüfen und gegebenenfalls auch weitergehende Auskünfte über sie einzuholen.

In der Praxis gestalten sich die (Pre-) Employment-Screenings zu Beginn sehr niederschwellig. Zunächst werden auf sozialen Netzwerken oder Karriereportalen Nachforschungen angestellt. Eine nachfolgende Steigerung liegt sodann oftmals im Abgleich mit Sanktionslisten oder Anti-Terror-Verordnungen.

Diese frühzeitigen Screenings setzen sich teilweise in bestehenden Arbeitsverhältnissen als sogenannte „Mitarbeiter-Screenings" fort.

Das Interesse des Arbeitgebers, so viel wie möglich über seine Arbeitnehmer (in spe) zu erfahren, ist zwar grundsätzlich nachvollziehbar, ist aus datenschutzrechtlicher Sicht aber kritisch zu betrachten. Diese Kritik greift insbesondere dann, wenn der Arbeitgeber keine klare gesetzliche Grundlage für die Screenings benennen kann. Dabei bestehen neben der DSGVO und dem BDSG dogmatisch viele Überschneidungen zum Arbeitsrecht. Insbesondere stehen die Screenings im Spannungsverhältnis zum „Recht zur Lüge" des Arbeitnehmers bei unzulässigen Fragen im Bewerbungsgespräch und zur Rechtsprechung der Arbeitsgerichte zum „Fragerecht des Arbeitgebers".

Gemeinsame Verantwortlichkeit nach Artikel 26 DSGVO

Das Konstrukt der gemeinsamen Verantwortlichkeit war bereits nach der alten Rechtslage der EG-Datenschutzrichtlinie bekannt, wurde dort aber nicht im Detail normiert. Die neue Regelung in Artikel 26 der DSGVO gestaltet diese Rechtsfigur nun ausdrücklich aus und formuliert explizite Vorgaben. Für die datenschutzrechtliche Praxis und die Gestaltung von Verträgen erlangt die gemeinsame Verantwortlichkeit damit umso größere Bedeutung. Wie die tägliche Arbeit meiner Behörde zeigt, ist die Abgrenzung der verschiedenen Formen datenschutzrechtlicher Verantwortlichkeit jedoch durchaus komplex, auch kann die Gestaltung entsprechender Verträge Verantwortliche vor Probleme stellen.

Anhand eines konkreten Projekts mit öffentlichen und privaten Stellen des Landes war es uns möglich, die für diese Abgrenzung relevanten Aspekte herauszuarbeiten und dadurch die zugehörigen Schwerpunkte für die Vertragsgestaltung zu identifizieren. So haben wir ein Vertragsmuster entworfen,

https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/05/190521_Vertragsmuster-Art-26.docx,

das durch eine Aufschlüsselung der verschiedenen Verarbeitungsprozesse in sogenannte Wirkbereiche im Einklang mit der aktuellen Rechtsprechung des EuGH zu den Voraussetzungen und Grenzen der gemeinsamen Verantwortlichkeit steht.

Durch genaue Zuordnung der Pflichten der einzelnen Verantwortlichen und transparente Bereitstellung aller notwendigen Informationen wird die Vorlage den Anforderungen des Artikels 26 DSGVO gerecht und verhilft den betroffenen Personen zu einem umfassenden Schutz ihrer

Rechte. Wir haben dieses Vertragsmuster bereits auf deutscher und europäischer Ebene öffentlich zur Verfügung gestellt und sogar in englischer Sprache herausgegeben. Hierdurch konnte eine allgemeintaugliche Praxishilfe geschaffen werden, um die grundlegenden Gesichtspunkte der gemeinsamen Verantwortlichkeit im Sinne des Artikels 26 DSGVO sinnvoll und praktikabel vertraglich zu gestalten.

Scoring

In Zeiten der Niedrigzinsen scheint es weit verbreitet, auf Pump zu kaufen und sich dadurch zu verschulden. Diese Einstellung bringt das Risiko der massiven Überschuldung mit sich. Das wiederum veranlasst die Unternehmen, sich vor Vertragsabschlüssen durch Einholen eines Score-Wertes von der Kreditwürdigkeit des Vertragspartners zu überzeugen. Dieser soll die Beurteilung des künftigen Zahlungsverhaltens der betroffenen Person ermöglichen. Score-Werte werden von Banken und Versicherungen vor dem Abschluss von Kredit- oder Versicherungsverträgen, aber auch von Vermietern im Zusammenhang mit Mietverträgen selbst berechnet oder bei Auskunfteien angefordert.

Dies kann im Rahmen von „Profiling" nach Art. 22 DSGVO dann zulässig sein, wenn ein Unternehmen eine automatisiert vorgenommene Bewertung für eine eigene maschinelle Entscheidung über den Abschluss oder die Erfüllung eines Vertrages nutzt (sog. internes Scoring) und dabei auch von einer Auskunftei angeforderte Score-Werte miteinbezieht. Auch nach BDSG darf, wer einen Vertrag schließen will, grundsätzlich bereits bei der Anbahnung des Geschäfts einen Score-Wert einholen (Art. 6 Abs. 1 lit. b DSGVO), sofern eine Reihe von Voraussetzungen erfüllt wird (§ 31 Abs. 1 BDSG).

Nicht abschließend geklärt sind derzeit Fragen der Reichweite von Betroffenenrechten, beispielsweise von Auskunftsrechten gegenüber Auskunfteien. Ein Anspruch besteht hier nicht nur auf die Kategorien von Daten, sondern auf konkrete Einzel-Daten, damit fehlerhafte Angaben noch vor ihrer Benutzung korrigiert und Missverständnisse aufgeklärt werden können. Umstritten ist, ob auch die Score-Formel selbst und die Gewichtung der einzelnen Angaben bzw. die statistischen Vergleichswerte mitgeteilt werden müssen, welche von Verantwortlichen gerne unter die Kategorie der Geschäftsgeheimnisse subsumiert werden. Wichtiger für Betroffene ist wohl die Erläuterung der Score-Berechnung. Nach jüngster Rechtsprechung zum Thema Bewertungsportale muss die Auskunftei beispielsweise mitteilen, welche Umstände maßgeblich dafür waren, dass die betroffene Person nicht als „uneingeschränkt kreditwürdig" bewertet wurde.

Spannend ist es hier, einen Blick durch die Brille des Informationsfreiheitsrechts zu werfen: Im Rahmen des Projektes „Open Schufa" hat die Open Knowledge Foundation durch den Aufbau einer Datenspende-Plattform zur Sammlung von Schufa-Einträgen versucht, den „Schufa-Code" nachzuvollziehen und gibt resümierend zumindest an, belegen zu können, dass die Schufa mit ihrer Auskunftspraxis gegen die DSGVO verstößt. Diese Aktion wurde für den Grimme-Preis nominiert.

Technischer Datenschutz

Bei allen Rechtsfragen stellt die technische Umsetzung der Forderungen der DSGVO Verantwortliche und Behörden immer wieder vor Probleme. Zahlreiche Meldungen von Datenpannen an meine Behörden wurden im vergangenen Jahr durch unser Technik-Referat ausgewertet.

Einige der größeren Datenpannen in Baden-Württemberg gingen auch durch die Presse: so beispielsweise die Hacking-Angriffe auf das Staatstheater Stuttgart und die Landesmesse Stuttgart. Themen wie Phishing, Erpressungstrojaner, Fernwartung sowie der Umgang mit Dienstleistern, die bei zahlreichen Datenpannen eine zentrale Rolle spielen, sind hier an der Tagesordnung.

Wie wir erfahren mussten, gibt es bei einigen Dienstleistern große Defizite im Hinblick auf die IT-Sicherheit. Dies hat bei Datenpannen enorme Auswirkungen auf personenbezogene Daten sehr vieler Betroffener. Außerdem sind in einigen Fällen auch die IT-Systeme der Kunden durch mangelnde Sicherheit der Dienstleister bedroht und führen zu massiven Problemen, beispielsweise durch Erpressungstrojaner.

Dies ist nur ein kleiner Ausschnitt aus dem Tätigkeitsfeld einer Datenschutz-Aufsichtsbehörde. Er mag als Beleg dafür dienen, dass die praktische und rechtliche Bedeutung des Datenschutzes sich in den kommenden Jahren eher noch steigern wird. Eine Folge davon ist, dass Datenschutz mittlerweile zum Kernbereich der Compliance-Bemühungen eines ▸

jeden Unternehmens zählt. Umso wichtiger, dass alle Verantwortlichen – Unternehmen, öffentliche Stellen und Aufsichtsbehörden – weiter im engen Austausch bleiben und so den Datenschutz „Made in Germany" gemeinsam fortentwickeln. Diese verstärkte Zusammenarbeit hat in den letzten Jahren einen guten Anfang genommen. Wir als Aufsichtsbehörden müssen und wollen auch künftig einen wesentlichen Beitrag hierzu leisten.

Weiterlesen

Zum Thema Recruiting unter der DSGVO finden Sie einen weiteren Beitrag in der Rubrik Datenschutz-Grundverordnung auf Seite 21.

Über den Autor

Dr. Stefan Brink
Landesbeauftragter für den Datenschutz
und die Informationsfreiheit Baden-Württemberg

www.baden-wuerttemberg.datenschutz.de

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Anzeige

DATENSCHUTZ | DIGITAL PRODUCT SECURITY | INFORMATIONSSICHERHEIT | IT-SECURITY

Online-eLearning Datenschutz / Informationssicherheit

Die einfachste Art zur Sensibilisierung und nachweislichen Schulung der Mitarbeiter

> sofort einsetzbar
> kostengünstig
> viele Sprachen

Bitte informieren Sie sich unter: https://elearning.ditis.de
Persönliche Beratung: Manfred Binder
Tel. 07321 37 7845, Manfred.Binder@ditis.de

ditis Systeme – Niederlassung der JMV GmbH & Co. KG • ein Unternehmen des Voith Konzerns
Lise-Meitner-Straße 15 • 89081 Ulm • www.ditis.de

DIE DATENSCHUTZBEAUFTRAGTEN, DIE DATENSCHUTZ-GRUNDVERORDNUNG UND DER BVD

Prof. Dr. Thomas Petri

Seit es in Deutschland Datenschutzgesetze gibt, gibt es die Diskussion um die betrieblichen Datenschutzbeauftragten. Kaum etabliert wurden sie immer wieder im Zusammenhang mit Bürokratieabbau in Verbindung gebracht. Die problematischen Auswirkungen des jüngst verabschiedeten 2. DSAnpUG EU auf den betrieblichen Datenschutz sind auch in diesem Heft bereits anderweitig beleuchtet worden, sodass ich hierauf näher nicht eingehen werde. Für mich interessant ist die Situation bei der Benennungspflicht von behördlichen Datenschutzbeauftragten.

Artikel 37 der EU-Datenschutz-Grundverordnung (DSGVO) sieht hinsichtlich der generellen Benennungspflicht von behördlichen Datenschutzbeauftragten keinen Gestaltungsspielraum der Mitgliedstaaten vor – und sie ist in Deutschland trotz vielfach vorhandener Finanznöte speziell von Kommunen auch nicht politisch infrage gestellt worden.

Wieso also sieht die DSGVO für öffentliche Stellen die Benennung eines Datenschutzbeauftragten verbindlich vor, obwohl sie an anderer Stelle sorgsam darauf bedacht ist, es den Mitgliedstaaten zu ermöglichen, ihre Behörden und öffentlichen Stellen von „bürokratischen Bürden“ zu entlasten? Und wieso ist der behördliche Datenschutzbeauftragte im öffentlichen Sektor als Institution politisch unumstritten?

Zur Beantwortung dieser Fragen hilfreich könnte insoweit ein Blick in die Vergangenheit sein. Schon § 14 Satz 2 BDSG 1977 sah vor, dass die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme “überwacht wird“. Viele Bundesbehörden erfüllten diese Überwachungspflicht, indem sie behördeninterne Datenschutzbeauftragte etablierten. Von Beginn des kodifizierten Datenschutzrechts an gibt es also behördliche Datenschutzbeauftragte, die sich um eine rechtskonforme personenbezogene Datenverarbeitung ihrer Einrichtung kümmern.

Heute unterscheidet die Datenschutz-Grundverordnung (EU) 2016/679 (DSGVO) kaum zwischen öffentlichen und nichtöffentlichen Stellen. ▸

Prof. Dr. Thomas Petri
Bayerischer Landesbeauftragte für den Datenschutz auf der Herbstkonferenz 2019 in Nürnberg
Foto: BvD e.V / Uli Schneider

Beim Datenschutzbeauftragten tut sie es ausnahmsweise. In Art. 18 Abs. 2 der Datenschutzrichtlinie 95/46/EG war dies noch anders. Sie sah die in anderen Mitgliedstaaten schon früher übliche Meldepflicht von Verarbeitungsverfahren vor. Von dieser bürokratischen Meldepflicht konnte das Recht der Mitgliedstaaten weitgehend entlasten, wenn es die Einrichtung eines internen Datenschutzbeauftragten vorsah. Eine Differenzierung zwischen öffentlichen oder nichtöffentlichen Stellen war dabei nicht vorgesehen. Die Mitgliedstaaten mussten die Benennung des internen Datenschutzbeauftragten auch nicht vorsehen, es war in ihr Belieben gestellt. Letztlich war das Institut des stelleninternen Datenschutzbeauftragten jedenfalls noch im Jahr 1995 als ein Modell der regulierten Selbstregulierung eine spezifisch deutsche Lösung, die in anderen Mitgliedstaaten selten zu finden war.

Jetzt hingegen sieht Artikel 37 Abs. 1 Buchstabe a) DSGVO ausdrücklich vor, dass jede Behörde und jede andere öffentliche Stelle einen Datenschutzbeauftragten zu benennen hat. Nichtöffentliche Stellen sind EU-rechtlich zur Benennung von betrieblichen Datenschutzbeauftragten nur unter den Voraussetzungen des Art. 37 Abs. 1 Buchstaben b oder c verpflichtet, wobei strengere mitgliedstaatliche Benennungspflichten möglich bleiben. Nachvollziehbare Gründe für die Unterscheidung zwischen einer Benennungspflicht von betrieblichen Datenschutzbeauftragten und behördlichen Datenschutzbeauftragten gibt es letztlich nicht. Ohne Zweifel würde der betriebliche Datenschutzbeauftragte auch in kleinen Unternehmen (nicht nur) zu einer Hebung des technisch-organisatorischen Datenschutzniveaus beitragen. Nach meiner persönlichen Überzeugung gäbe es auch im Datenschutzrecht andere, effektivere Wege, um kleine Unternehmen von „bürokratischen Bürden" zu befreien.

Erklärtes Ziel im Vorschlag einer Datenschutz-Grundverordnung (KOM (2012), 0011 endg. = Bundesrats-Drucksache 52/12, S. 5) war eine *Verwaltungsvereinfachung* – also eine Entschlackung des Datenschutzrechts von überflüssigen bürokratischen Erfordernissen. Ganz offenbar hatte die Kommission bei ihrer Evaluation der Datenschutzrichtlinie 95/46/EG den Eindruck gewonnen, dass die Benennung von Datenschutzbeauftragten diesem Ziel gerade nicht abträglich, sondern vielmehr zur Hebung des Datenschutzniveaus förderlich sei. Im Gesetzgebungsverfahren wurde der Vorschlag der Kommission in diesem Punkt auch kaum diskutiert. Im Europäischen Parlament gab es zwar vereinzelte Änderungsanträge auch zur Benennung von behördlichen Datenschutzbeauftragten, die Diskussion hierzu verlief jedoch nicht ansatzweise so kontrovers wie hinsichtlich der Benennungsvoraussetzungen für die betrieblichen Datenschutzbeauftragten. Entsprechendes galt für die Willensbildung im Rat.

Die Entstehungsgeschichte des Art. 37 DSGVO gibt also letztlich keine eindeutige Antwort auf die eingangs gestellten Fragen nach dem Grund für eine generelle Benennungspflicht für öffentliche Stellen. Könnte ein Blick auf den Vollzug der stelleninternen Kontrolle weiterhelfen? Die Antwort lautet aus Sicht einer Datenschutzaufsichtsbehörde eindeutig: ja. Das Modell des oder der behördlichen Datenschutzbeauftragten hat sich hervorragend bewährt. Bereits der Umstand, dass „jemand da" ist, der die Funktion eines Ansprechpartners und Beratungsinstanz wahrnimmt, führt erfahrungsgemäß zu einem qualitativ höheren Datenschutzbewusstsein. Was speziell die behördlichen Datenschutzbeauftragten anbelangt: Die Verarbeitung personenbezogener Daten im öffentlichen Interesse ist eine komplexe Rechtsmaterie. Auf der Vollzugsebene sind nicht nur mehrere Gesetzesebenen

(EU-Recht, Bundes- und Landesrecht, teilweise auch kommunales Recht) in das richtige Verhältnis zu setzen. Zu berücksichtigen sind auch fachrechtliche Besonderheiten, die datenschutzrechtlich ihren Niederschlag finden. Zugleich ist es wichtig, dass eine interne Kontroll- und Beratungsinstanz mit den Besonderheiten der öffentlichen Verwaltung hinreichend vertraut ist. Vor diesem Hintergrund ist es gut, wenn es Datenschutzbeauftragte gibt, die den Verantwortlichen kompetent dabei unterstützen, die Einhaltung der Datenschutzbestimmungen zu überwachen (siehe auch Erwägungsgrund 75 DS-GVO). Vor dem Hintergrund der technisch-organisatorischen Vorgaben an ein Datenschutzmanagement tragen Datenschutzbeauftragte gerade auch bei kleineren Behörden oft ganz erheblich dazu, dass die technischen Verarbeitungsprozesse nicht nur „compliant" sind, sondern auch noch gut funktionieren.

Als Ergebnis lässt sich also festhalten: Die stelleninternen Datenschutzbeauftragten haben sich als interne Kontroll- und Beratungsinstanz verantwortlicher Stellen bestens bewährt. Deshalb freut es mich, dass der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. die Arbeit der behördlichen Datenschutzbeauftragten in Bayern unter anderem durch Informationsveranstaltungen wie den „Behördentag 2019" unterstützt. Allen behördlichen Datenschutzbeauftragten, die täglich – zum Teil unter schwierigen Bedingungen – dazu beitragen, dass der Freistaat Bayern auch unter dem Gesichtspunkt des Persönlichkeitsrechts ein lebenswertes Land ist und bleibt, sei bei dieser Gelegenheit herzlich gedankt!

Über den Autor

Prof. Dr. Thomas Petri
ist seit Juli 2009 Bayerischer Landesbeauftragte für den Datenschutz

▶ www.datenschutz-bayern.de

Anzeige

- Interne & externe Datenschutzbeauftragte -

Sie suchen eine Haftpflicht-Versicherung? Sie möchten Ihre bestehende Police vergleichen?

Berufs-Haftpflichtversicherung für interne und externe DSB – in Zusammenarbeit mit dem BvD entwickelt

Als Berater schützen Sie Unternehmen vor Haftungsansprüchen - wir schützen Sie.

- exclusives Wording für BvD-Mitglieder (auf Berufsbild DSB zugeschnitten)
- Tätigkeit ‚Auditor für Datenschutz' beitragsfrei eingeschlossen
- niedrige Einsteigerprämie sowie professionelle Beratung

- inkl. DS-GVO
- hohe Deckungssummen zu verbesserten Konditionen

Für nähere Informationen rufen Sie uns gerne an: 06174 - 96843-0 oder unter www.bvdnet.de (Mitgliederbereich)

Butz - Versicherungsmakler GmbH Ansprechpartner: Herr Jared Butz Tel: 06174 - 96843-0 Fax: 06174 - 96843-29
info@butz-versicherungsmakler.de www.butz-versicherungsmakler.de

BUßGELDBEMESSUNG: SO GEHEN DIE AUFSICHTSBEHÖRDEN KÜNFTIG VOR

Dr. Jens Eckhardt

Anfang September haben Meldungen auf dem Newsportal juve.de Wirbel zu einem Bußgeldberechnungsmodell der Datenschutzaufsichtsbehörden ausgelöst. Fast zeitgleich wurde schon die Möglichkeit zur Berechnung von Bußgelder (Stichwort: elektronische Bußgeldrechner) beworben. Am 16. Oktober veröffentlichten die deutschen Datenschutzaufsichtsbehörden ihren ersten Aufschlag zur Berechnung von Bußgeldern. Lassen sich Bußgelder zukünftig durch einen automatischen „Bußgeldrechner" bestimmen? Sicherlich nicht – Art. 83 DSGVO steht dem entgegen, da er Kriterien vorsieht, die sich nicht abstrakt „verformeln" lassen. Und: Haben die Aufsichtsbehörden überhaupt eine solche rein mathematische Berechnung vorgesehen?

Der Hintergrund

Die DSGVO sieht hohe Bußgelder vor. Es ist eine einfache Überlegung, dass ein Bußgeldrahmen bis zu 20 Millionen Euro oder bis zu vier Prozent des weltweiten Vorjahresumsatzes eines Unternehmensverbunds mehr Spielräume für die Bemessung bietet, als der bisherige Bußgeldrahmen. Damit wird es aber auch schwieriger, das „richtige" Bußgeld zu finden. Und vor allem unangreifbar zu begründen. Denn je kleiner das Bußgeld, umso höher die Bereitschaft es zur „Beendigung des Themas" zu akzeptieren.

Die DSGVO gibt in Art. 83 Abs. 2 DSGVO eine Reihe von Kriterien für die Bemessung eines Bußgelds vor. Eine Befassung mit diesen Kriterien – auch unter Heranziehung der „Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679" (WP 253) der Art.-29-Gruppe vom 03.10.2017 – wirft auch die Frage auf, ob diese Kriterien die Bemessung wirklich leichter machen. Daraus ergeben sich zwar Anhaltspunkte für die Bewertung, aber der eingangs angesprochene Spielraum ist immer noch recht weit.

Weitere Anhaltspunkte sieht die DSGVO selbst nicht vor. Die Verweise des deutschen BDSG auf das Ordnungswidrigkeitenrecht führen zwar zur Anwendung des „deutschen Verfahrensrechts", aber nicht zwingend zur Anwendung der deutschen Bemessungsregeln (vgl. § 41 Abs. 1 Satz 2 BDSG). Gleichwohl erscheinen die Überlegungen des Ordnungswidrigkeitenrechts nicht vollkommen abwegig, den vollen Bußgeldrahmen für vorsätzliche Taten anzuwenden und den halben Bußgeldrahmen bei fahrlässigen Taten (vgl. § 17 Abs. 2 OWiG). Ausgehend von diesem Rahmen kann für einen durchschnittlichen Verstoß der jeweilige Mittelwert angesetzt und anhand der Bemessungskriterien erhöht oder gesenkt werden. Allerdings sind damit die zuvor angesprochenen Probleme nicht gelöst. Hinzu kommt, dass die Anwendung EU-weit einheitlich erfolgen muss, da die DSGVO EU-weit einheitlich ausgelegt und gehandhabt werden muss.

Ein Blick auf die bisher veröffentlichten Bußgelder in Deutschland und anderer EU-Mitgliedstaaten vermittelt durchaus den Eindruck, dass die deutschen Aufsichtsbehörden einen eher moderaten Ansatz wählen. Der Eindruck kann jedoch täuschen, denn über die unterschiedlichen Sachverhalte und die Umstände der Verhängung der Bußgelder ist schlicht nicht genug bekannt.

Da in Deutschland nicht erstmalig mit der DSGVO Sanktionen für Verstöße eingeführt worden sind, mag es auf den ersten Blick verwundern, dass die Bemessung in Deutschland so schwer sein soll. Allerdings lässt der Bußgeldrahmen viel Spielraum und die Kriterien zur Bußgeldbemessung sind vom Start weg eher scheinbare als echte Hilfen. Aus rechtsstaatlichen Gründen verbietet sich aber ein „Auswürfeln" der Bußgeldhöhe.

Das Berechnungsmodell

Nachdem bei juve.de am 6. September ein Artikel zu einem Bußgeldmodell der Aufsichtsbehörden erschienen war, reagierte die Datenschutzkonferenz (DSK) mit einer Pressemitteilung am 17. September. Sie bestätigte die Arbeit an einem Bußgeldmodell und stellte eine Veröffentlichung für November in Aussicht. Bereits am 16. Oktober veröffentlichte die DSK dann ihren Ansatz zur Festlegung von Bußgeldern mit dem Titel „Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen". Der Pressemitteilung der DSK ist hierzu unter anderem das Folgende zu entnehmen: Mit der Veröffentlichung der vorliegenden Fassung des Konzeptes zur Bemessung von Geldbußen soll ein Beitrag zur Transparenz im Hinblick auf

die Durchsetzung des Datenschutzrechts geleistet werden. Es soll Verantwortliche und Auftragsverarbeiter in die Lage versetzen, die Entscheidungen der Aufsichtsbehörden nachzuvollziehen. Das Konzept unterstützt mit der Anknüpfung an den Umsatz eines Unternehmens bei der Bußgeldzumessung den erklärten Willen des europäischen Gesetzgebers, die Wirksamkeit, Verhältnismäßigkeit und abschreckende Wirkung der Verhängung von Geldbußen sicherzustellen.

Das veröffentlichte Modell zur Bestimmung des Bußgelds wird nur bei Bußgeldern gegen Unternehmen angewendet und erfolgt in fünf Schritten:

Schritt 1: Zuordnung des Unternehmens zu einer Größenklassen

Dem Konzept ist hierzu unter anderem Folgendes zu entnehmen: Die Größenklassen richten sich nach dem gesamten weltweit erzielten Vorjahresumsatz der Unternehmen (vgl. Art. 83 Abs. 4 bis 6 DSGVO) und sind unterteilt in Kleinstunternehmen, kleine und mittlere Unternehmen (KMU) sowie Großunternehmen. Es gilt gemäß Erwägungsgrund 150 der DSGVO der Begriff „Unternehmen" im Sinne der Artikel 101 und 102 AEUV (sog. funktionaler Unternehmensbegriff). Die Größeneinordnung der KMU orientiert sich hinsichtlich des Vorjahresumsatzes grundsätzlich an der Empfehlung der Kommission vom 6. Mai 2003 (2003/361/EG).

Die Größenklassen A (Jahresumsatz bis zwei Millionen Euro), B (Jahresumsatz über zwei und bis zehn Millionen Euro), C (Jahresumsatz über zehn und bis 50 Millionen Euro) und D (Jahresumsatz über 50 Millionen Euro) werden wiederum zur konkreteren Einordnung der Unternehmen nochmals in Untergruppen unterteilt (A.I bis A.III, B.I bis B.III, C.I bis C.VII, D.I bis D.VII).

Damit ergeben sich insgesamt 20 Kategorien, die im Konzept tabellarisch benannt sind.

Schritt 2: Ermittlung des mittleren Jahresumsatzes der jeweiligen Untergruppe

Dieser Wert ist der Tabelle 2 des Konzepts zu entnehmen und dient der Veranschaulichung der in den folgenden Schritten darauf aufbauenden Ermittlung des wirtschaftlichen Grundwerts.

Dieser Ausgangswert ist in der niedrigsten Gruppe A. I. (also bei einem Jahresumsatz bis 700.000 Euro) 350.000,00 € und in der höchsten Gruppe D. VII. (also Jahresumsatz des Unternehmens von mehr als 500 Mio. €) der konkrete Jahresumsatz des Unternehmens.

Schritt 3: Ermittlung des wirtschaftlichen Grundwerts

Für die Festsetzung des wirtschaftlichen Grundwerts wird der mittlere Jahresumsatz der Untergruppe (Schritt 2), in die das Unternehmen eingeordnet wurde, durch 360 Tage geteilt und so ein durchschnittlicher, auf die Vorkommastelle aufgerundeter Tagessatz errechnet. Dieser ist der Tabelle 3 des Konzepts zu entnehmen.

Dieser Grundwert ist in der niedrigsten Gruppe A. I. (also Jahresumsatz bis 700.000 Euro) 972,00 Euro und in der höchsten Gruppe D. VII. (also Jahresumsatz des Unternehmens von mehr als 500 Mio. €) der konkret errechnete Tagessatz. Zur Verdeutlichung in der zweiten höchsten Gruppe D. VI. (Jahresumsatz über 400 bis 500 Millionen Euro) sind das 1,25 Millionen Euro.

Schritt 4: Multiplikation des Grundwerts mittels eines von der Schwere der Tatumstände abhängigen Faktors

Erstmals in Schritt 4 erfolgt anhand der konkreten tatbezogenen Umstände des Einzelfalls eine Einordnung des Schweregrads der Tat in leicht, mittel, schwer oder sehr schwer. Hierfür werden gemäß der Tabelle 4 des Konzepts unter Berücksichtigung der Umstände des Einzelfalls anhand des Kriterienkatalogs des Art. 83 Abs. 2 DSGVO der Schweregrad des Tatvorwurfs und damit der jeweilige Multiplikationsfaktor ermittelt. Mit diesem soll der (in Schritt 3 ermittelte) Grundwert multipliziert werden.

Aufgrund der unterschiedlichen Bußgeldrahmen wird zwischen Verstößen gegen formelle Regelungen (Art. 83 Abs. 4 DSGVO) und materielle Regelungen der DSGVO (Art. 83 Abs. 5, 6 DSGVO) unterschieden und in zwei Spalten der Tabelle unterschiedliche Faktoren festgelegt. Die in vier Abstufungen vorgesehenen Multiplikatoren sind bei „formellen Verstößen" 1 bis 6 und bei „materiellen Verstößen" 1 bis 12. Bei der Wahl des Multiplikationsfaktors einer sehr schweren Tat ist – so das Konzept – zu beachten, dass der einzelfallbezogene Bußgeldrahmen nicht überschritten wird.

Schritt 5: Anpassung des in Schritt 4 ermittelten Werts anhand täterbezogener und sonstiger noch nicht berücksichtigter Umstände

Der in Schritt 4 berechnete Betrag wird anhand aller für und gegen das Unternehmen sprechenden Umstände angepasst, soweit diese noch nicht in Schritt 4 berücksichtigt wurden. Das sollen insbesondere sämtliche täterbezogenen Umstände des Kriterienkatalogs in Art. 83 Abs. 2 DSGVO ▸

sowie sonstige Umstände wie eine lange Verfahrensdauer oder eine drohende Zahlungsunfähigkeit des Unternehmens sein.

Eine erste Einschätzung

Dieses Berechnungsmodell macht zunächst plakativ deutlich, was der neue Bußgeldrahmen der DSGVO in der Praxis bedeuten kann – aber nicht zwingend muss.

Trotz aller hierzu bereits veröffentlichten Kritik muss gesehen werden, dass die Aufsichtsbehörden damit versuchen, in die Berechnung Transparenz zu bringen und damit auch für eine gewisse Gleichheit zu sorgen – sowohl nach oben als auch nach unten. Solche Tabellen und Schemen sind in der Praxis der Sanktionierung auch nicht unüblich.

Für den mit der Verteidigung in Bußgeldsachen befassten Rechtsanwalt drängt sich zunächst der Impuls auf, dass die Aufsichtsbehörde allein aufgrund der Konzeption des Modells (zuerst Berechnung des „Tagessatzes" und erst anschließende „tat- und schuldangemessene Bewertung") zu einem anderen Ergebnis kommt, als wenn zuerst Tat und Schuld gewichtet würden. Bei rein mathematischer Betrachtung ergibt sich vielleicht kein Unterschied allein danach, was zunächst festgelegt wird. In der Praxis besteht dennoch die Gefahr, dass beim vorgestellten Vorgehen tendenziell höhere Bußgelder das Ergebnis sind.

Erste Kritikpunkte sind der Umstand, dass die Heranziehung eines Durchschnittswerts in Schritt 2 diejenigen benachteiligt, die an der unteren Grenze der jeweiligen Gruppe stehen, ein Aspekt, der in Schritt 5 „abgefedert" werden muss. Der Umsatz als Einstieg in eine Bewertung birgt auch die Gefahr, dass margenschwache Unternehmen (Stichwort: hoher Umsatz, aber geringer Gewinn) benachteiligt werden könnten. Denn wenn zuerst eine tat- und schuldbezogene Bewertung erfolgen würde mit anschließender Multiplikation mit einem Tagessatz, liegt es in der Praxis nahe, dass ein geringerer Wert zur Diskussion stünde. Ein Aspekt, der ebenfalls stark in Schritt 5 berücksichtigt werden muss.

Ein wesentlicher Kritikpunkt ist, dass in den Schritten 1 bis 3 kein Wert für einen mittleren Verstoß berechnet wird, von dem ausgehend dann schuld- und tatangemessen Ab- und Aufschläge gebildet werden, sondern ein Mindestwert festgelegt ist. In Schritt 4 sind nur erhöhende Multiplikatoren vorgesehen. Erst in Schritt 5 ist vorgesehen, dass auch Abstriche von dem bis dahin ermittelten Wert möglich sind. Hierdurch entsteht ein Störgefühl, dessen Berechtigung weitergehend hinterfragt und untersucht werden muss.

Die Aufteilung in fünf Schritte, wovon die ersten drei „nur" Rechenschritte sind, führt wohl beim ersten Lesen zu dem Eindruck, dass sich Bußgelder mathematisch berechnen lassen und die Sanktion sich allein dadurch finden lässt. Das ist aber in erster Linie des Umfangs dieser ersten drei Schritte im Vergleich zu den letzten beiden geschuldet. In der Sache machen die Schritte 4 und 5 deutlich, dass sich ein Bußgeld nicht rein mathematisch errechnen lässt, sondern Gewichtungen eine erhebliche Bedeutung haben (müssen).

Wenn die erste Überraschung – vielleicht auch der erste Schreck – verflogen ist, wird sich zeigen, dass die Schritte 4 und 5 weiterhin eine signifikante Rolle spielen werden. Hier erfolgt die tat- und schuldangemessene Bußgeldbemessung. Auch die Aufsichtsbehörden scheinen dies nicht zwingend anders zu sehen. Denn diese individuellen Aspekte werden nicht vernachlässigt. Auch bleiben all die Schwierigkeiten im Umgang mit den Kriterien in Schritt 4 und 5. Gerade die entscheidenden Aspekte lassen sich durch Bußgeldrechner nicht abbilden.

Aus der Sicht der Verteidigung gegen Bußgelder besteht in gewisser Weise das Gefühl, gegen einen hohen Ausgangswert „ankämpfen" zu müssen. Zu sehen ist dabei aber, dass die Auswahl des Multiplikators in Schritt 4 schon nicht mehr rein mathematisch erfolgen kann. Gerade in den Schritten 4 und 5 wird zukünftig (wie bisher) die „Musik spielen". Natürlich wird auch das Berechnungsmodell (im Einzelfall und generell) nicht kritiklos bleiben (können).

Nicht übersehen werden darf, dass die beste Verteidigung gegen ein Bußgeld darin besteht, möglichst keinen schuldhaften oder jedenfalls keinen sanktionswürdigen Verstoß zu begehen. In der Praxis beginnt schon hier die Verteidigung gegen ein Bußgeld und gerade an diesem Punkt können die Unternehmen durch Datenschutz-Compliance ihr Bußgeld-Risiko im Vorfeld reduzieren.

Über den Autor

Dr. Jens Eckhardt
Vorstands-Mitglied des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V.
sowie Rechtsanwalt und Fachanwalt für IT-Recht bei dmp Derra, Meyer & Partner PartGmbB, Düsseldorf, Ulm, Berlin

DATENSCHUTZVORFÄLLE – EIN ERFAHRUNGSBERICHT NACH EINEINHALB JAHREN DSGVO

Thomas Kahl

Die IT-Sicherheitslage der Nation scheint prekär: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) konstatiert in seinem aktuellen Bericht zur Lage der IT-Sicherheit in Deutschland für 2019 nach wie vor eine angespannte IT-Sicherheitslage wie eine weiterhin hohe Dynamik der Angreifer bei der (Weiter-)Entwicklung von Schadprogrammen und Angriffswegen.

Unzählige Unternehmen sind seit Inkrafttreten der DSGVO Opfer von Cyber-Angriffen wie zum Beispiel der letzten großen Angriffswelle mit der Schadsoftware Emotet geworden.

Der nachfolgende Beitrag soll einen Einblick liefern, welche Fragestellungen in der Beratungspraxis bei Cyberangriffen seit dem 25. Mai 2018 besonders relevant waren und was die Lessons Learned sind, die Unternehmen in Zukunft beachten sollten.

Datenschutzvorfälle – Eine große rechtliche wie praktische Herausforderung

Die rechtliche Beratung von Unternehmen im Fall von Cyberangriffen ist regelmäßig durch große rechtliche wie praktische Herausforderungen gekennzeichnet. Zum einen führen die vielfach unklaren rechtlichen Vorgaben der DSGVO und des BDSG zu erheblicher Unsicherheit für betroffene Unternehmen bei der Bewertung der Meldepflichtigkeit einzelner Vorgänge.

Zudem sehen sich Unternehmen im Fall eines Cyberangriffs meist mit der Herausforderung konfrontiert, auf Basis einer unklaren Tatsachenlage in kürzester Zeit rechtlich weitreichende Entscheidungen wie etwa über die Meldung eines Vorgangs an die zuständige Aufsichtsbehörde treffen zu müssen.

Besondere Relevanz erlangen diese Umstände nicht zuletzt durch die erhebliche Bußgeldandrohung nach der DSGVO. Denn auch unzureichendee technisch organisatorische Maßnahmen oder eine „bloß“ unterlassene Meldung können zu erheblichen Sanktionen führen.

Hinzu kommt, dass – für viele Unternehmen oft unbekannt – eine Vielzahl weiterer Gesetze Vorgaben zum Thema Cyber-Security beinhalten. Dazu gehören das Telemediengesetz (TMG) und das Telekommunikationsgesetz (TKG).

Aber auch auf den ersten Blick eher „unverdächtige“ Gesetze verpflichten ausdrücklich oder zumindest implizit zur Einhaltung entsprechender Standards, wie das Handelsgesetzbuch (HGB), das GmbH-Gesetz (GmbHG) oder das Aktiengesetz (AktG).

Danach ist die IT-Sicherheit Teil der wesentlichen Aufgaben der Unternehmensleitung, die die Verantwortung für die Umsetzung der erforderlichen IT-Sicherheitsmaßnahmen trifft. Erfolgt das nicht, kann die Geschäftsleitung hierfür persönlich verantwortlich gemacht werden. Denn für ausreichende IT-Sicherheit zu sorgen, gehört zu den wesentlichen Grundsätzen der ordnungsgemäßen Geschäftsführung.

Ergo: Die Gefahr durch Cyber-Attacken ist nicht nur wegen der DSGVO ein Thema für das Risikomanagement eines jeden Unternehmens!

Drei Fragen aus der Beratungspraxis, die sich immer wieder stellen

Blickt man auf die ersten knapp 1,5 Jahre der Beratung entsprechender Vorgänge unter der DSGVO, fallen einige immer wiederkehrende und besonders relevante Fragestellungen ins Auge, die sich in nahezu allen Fällen stellen – insbesondere zu den Vorgaben aus Art. 33, 34 DSGVO. Dabei zeigt die hohe Zahl der bei den Aufsichtsbehörden eingehenden Meldungen gemäß Art. 33 DSGVO, dass Behörden wie betroffene Unternehmen bei der Interpretation der Vorgaben nach Art. 33 DSGVO ein weites Begriffsverständnis zu Grunde zu legen scheinen. Eine Entwicklung, die es sinnvoll erscheinen lässt, ▸

die Interpretation der Art. 33, 34 DSGVO in der Behördenpraxis noch einmal auf den Prüfstand zu stellen, um eine möglichst einheitliche Anwendung der Vorgaben in der EU sicherzustellen.

Melden macht frei … oder vielleicht doch nicht?

Die wohl vordringlichste Frage aus Sicht betroffener Unternehmen ist regelmäßig die nach der Meldepflicht eines konkreten Vorgangs gemäß Art. 33 DSGVO. Die Praxis zeigt, dass viele Unternehmen Vorgänge melden, die zumindest auf den zweiten Blick der Meldepflicht des Art. 33 DSGVO vielleicht gar nicht unterfallen. Zudem werden oftmals viele Informationen preisgegeben, die nicht zwingend zum Gegenstand einer Meldung zu machen sind.

Diese Praxis mag in vielen Fällen keine negativen Konsequenzen für die betroffenen Unternehmen nach sich ziehen. In Fällen, in denen Unternehmen jedoch nicht so ordentlich beim Datenschutz aufgestellt sind, der Datenschutzvorfall durch Fehler des betroffenen Unternehmens erzeugt wurde oder eine Meldung ohne ausreichende Begründung verspätet erfolgt, kann die Frage der Meldepflicht in einem anschließenden Verwaltungs- oder Bußgeldverfahren jedoch enorme Bedeutung erlangen.

Denn ob melden tatsächlich in jedem Fall „frei macht", darf zumindest rechtlich bezweifelt werden. Die Reichweite des Beweisverwertungsverbotes gemäß § 42 Abs. 4 BDSG scheint ungeklärt. Dass ein Unternehmen durch eine entsprechende Meldung stets einen „Freifahrtschein" erhält, scheint eher unwahrscheinlich. Zudem scheinen verschiedene Aufsichtsbehörden die Vorgaben unterschiedlich zu interpretieren, so dass eine Meldung in einem Bundesland je nach Vorgang andere Folgen haben könnte als in einem anderen Bundesland.

In jedem Fall sollte einer Meldung somit sorgfältig Prüfung der Tatbestandsvoraussetzungen vorausgehen. Zudem sollte genau geprüft werden, welche Tatsachen zu melden sind – und welche nicht. Wenn die rechtliche Einschätzung es erlaubt, dürfte auf Grund der mit einer Meldung einhergehenden Risiken zukünftig durchaus mehr Zurückhaltung geboten sein, als dies in der gegenwärtigen Praxis zu beobachten ist.

Wann liegt eine „Datenschutzverletzung" gemäß Art. 33 DSGVO vor?

Unklarheiten scheinen in der Praxis gleichfalls zu bestehen, wenn es darum geht, eine „Datenschutzverletzung" gemäß Art. 33 DSGVO festzustellen. Fälle, die hier oftmals für Nachfragen sorgen sind solche, in denen zwar personenbezogene Daten unzulässig verarbeitet wurden, dies aber zumindest nicht unmittelbar auf eine Verletzung technischer Schutzmaßnahmen zurückzuführen ist, also wenn beispielsweise keine Passwörter geknackt oder Systeme eines Unternehmens mit technischen Mitteln wie einer Schadsoftware kompromittiert wurden. Zu nennen sind hier Fälle des sogenannten Social Engeneerings, bei dem beispielsweise ein Mitarbeiter eines Unternehmens durch Manipulation wie der Verschleierung der wahren Identität einer Person zu einer Handlung verleitet wird. In entsprechenden Fällen dürfte oftmals kritisch zu hinterfragen sein, ob die für einen Datenschutzvorfall gemäß Art. 33 DSGVO erforderliche

Verletzung der „Sicherheit“ i.S.d. Art. 4 Nr. 12 DSGVO tatsächlich gegeben ist. Die Melde- und Behördenpraxis zeigt, dass hier oftmals ein weites – aus Sicht des Verfassers tendentiell zu weites – Begriffsverständnis des Art. 33 DSGVO zu Grunde gelegt wird.

Die „Risikoprognose“ gemäß Art. 33 und 34 DSGVO – Wann liegt ein (hohes) Risiko vor?

Handelt es sich dem Grunde nach um einen meldepflichtigen Vorgang, bedarf es der Feststellung eines entsprechenden Risikos für die Betroffenen i.S.d. Art. 33 DSGVO, um die Meldepflicht auszulösen. Da insbesondere Cyber-Angriffe oft von dem Umstand gekennzeichnet sind, dass sich schwer bis kaum bestimmen lässt, ob personenbezogene Daten tatsächlich kompromittiert wurden, ist die Entscheidung über die Meldung regelmäßig im Wege einer Risikoprognose zu treffen. Diese Prognose hat sich insbesondere an der Sensitivität der potentiell betroffenen Daten, der sich daraus ergebenden (potentiellen) Schwere etwaiger Nachteile für die betroffenen Datensubjekte sowie der Eintrittswahrscheinlichkeit zu orientieren. So kann in einem Fall, in dem der tatsächliche Zugriff eines Angreifers auf personenbezogene Daten unklar ist, jedoch hoch-sensitive Daten (z.B. Patientendaten) betroffen sind, eine Meldung angezeigt sein, bei weniger sensitiven Daten (z.B. bloße Kontaktdaten) dagegen im Zweifel nicht.

Fraglich scheint die Einordnung insbesondere in Fällen, in denen sich die Risiken eher als solche für das betroffene Unternehmen und weniger für eine betroffene Person (z.B. einen Mitarbeiter) herausstellen. Dabei ist sicherlich fraglich, ob die bloße Kenntnisnahme von geschäftlichen Kontaktdaten eines Mitarbeiters durch unberechtigte Dritte im Rahmen eines Cyberangriffs tatsächlich ein Risiko für die Betroffenen gemäß Art. 33 DSGVO auslösen kann. Hier wird es aber sicher stets einer individuellen Betrachtung der Einzelfälle bedürfen.

Angesichts der im Vergleich zu anderen EU-Ländern enorm hohen Zahlen der seit dem 25. Mai 2018 bei den Behörden in Deutschland eingegangener Meldungen, sollte die Meldepraxis und Interpretation dieser und anderer Tatbestandsmerkmale des Art. 33 DSGVO nochmals auf den Prüfstand gestellt werden.

Lessons Learned – Drei Maßnahmen, um sich auf den Ernstfall vorbereiten

Schon vor einem möglichen Vorfall können sich Unternehmen auf den Ernstfall vorbereiten. Neben der Implementierung ausreichender Maßnahmen zur Datensicherheit sind regelmäßig weitere Schritte erforderlich, um sich für den Ernstfall zu rüsten. Hier eine kleine Auswahl möglicher Vorabmaßnahmen, die jedes Unternehmen prüfen sollte:

1. Jedes Unternehmen sollte sich einen „Krisenplan“ zurechtlegen, mit dem im Krisenfall die wichtigsten Schritte schnell und effektiv abgearbeitet werden können. Wesentliche Punkte eines solchen Plans sind:

- Festlegung von Verantwortlichkeiten
- Eskalationswege zur Einbindung der Geschäftsleitung, des DSB, der Rechtsabteilung und anderen Entscheidungsträgern
- Ausarbeitung von Ablaufplänen und Sofortmaßnahmen
- Implementierung eines Systems zur internen Meldung entsprechender Vorfälle inklusive Templates zur Meldung und Dokumentation von Vorfällen

Ein entsprechender Krisenplan für IT-Sicherheitsvorfälle ist ausreichend zu dokumentieren und sollte in regelmäßigen Abständen im Wege einer Simulation erprobt werden.

Ein solcher Plan ist nicht nur „nice to have“. Vielmehr sind Unternehmen bereits auf Grund der Vorgaben der DSGVO sowie – oftmals unbekannt – aus gesellschaftsrechtlichen Vorgaben verpflichtet, entsprechende Maßnahmen als Teil eines funktionierenden Business Continuity Managements zu treffen.

2. Jedes Unternehmen sollte ein Team externer Experten bestimmten, die im Angriffsfall schnell unterstützen können. Zum Team sollten IT-, Rechts- und Kommunikationsfachleute gehören. Externe Hilfe kann im Fall eines Cyberangriffs eine wertvolle Ergänzung zum internen Krisenmanagement darstellen. In diesem Zuge sollten Unternehmen die relevanten Anlaufstellen bei den zuständigen Behörden definieren, um etwaige Meldungen rechtzeitig durchführen zu können

3. Unternehmen, die beim Datenschutz ggf. nicht so gut aufgestellt sind, sollten mit Priorität alle leicht zu entdeckenden „Datenschutzfehler“ beseitigen, wofür im Fall eines Datenschutzvorfalls oft wenig Zeit bleibt. Überprüft werden sollte in diesem Zuge zunächst die Datenschutzstrategie für Websites und Mobile Apps. Datenschutzhinweise sind zu prüfen und nachzubessern.

Die Verschlüsselungen der Webseitenkommunikation ist auf einen sicheren Stand zu bringen. Zuletzt ist der Datenschutzbeauftragte ordnungsgemäß an die zuständige Behörde zu melden. Entsprechende Maßnahmen sind enorm wichtig, da diese als *„Low Hanging Fruits“* gern ▸

durch Aufsichtsbehörden im Fall einer Meldung gem. Art. 33 DSGVO geprüft werden, um such schnell einen Eindruck von der Datenschutzsituation des Unternehmens zu verschaffen.

Fazit

Datenschutzvorfälle stellen die Beteiligten vor große praktische wie rechtliche Herausforderungen. Wie so oft liegt in der Ruhe aber auch die Kraft – nicht zuletzt, um in der Hektik Fehler zu vermeiden, die später weitreichende Folgen haben können. So können unachtsame oder voreilige Meldungen im Ernstfall zu aufsichtsbehördlichen Verfahren und Sanktionen führen, gegen die sich das Unternehmen nur noch bedingt verteidigen kann. Voreilige und ungeprüfte interne Ermittlungsmaßnahmen können weitere Datenschutzverstöße und Beweisverwertungsverbote zur Folge haben. Externe Berater können helfen, Fehler zu vermeiden und etwaige Themen als Außenstehende objektiv und unbefangen zu betrachten. Ungeachtet dessen und bei aller Kritik einer womöglich zu weit geratenen Interpretation der Vorgaben des Art. 33 DSGVO gilt auch hier, dass ein kooperatives Zusammenarbeiten mit den zuständigen Aufsichtsbehörden sich bezahlt machen kann. Das sollte bei all den Diskussionen rund um das „richtige" Verhalten bei Datenschutzvorfällen nie aus dem Auge verloren werden.

Über die Autoren

Thomas Kahl
Fachanwalt für IT-Recht, Taylor Wessing
Der Autor ist Rechtsanwalt und Salary Partner der internationalen Wirtschaftskanzlei Taylor Wessing am Standort Frankfurt. Er berät nationale wie internationale Unternehmen zu Fragen des Datenschutzes, der IT-Sicherheit und Compliance im Rahmen der Ausgestaltung von (konzernweiten) Datenverarbeitungsprozessen und aufsichtsbehördlichen Verfahren.

▶ www.taylorwessing.com

TaylorWessing

Anzeige

RHENUS DATA OFFICE GMBH

RHENUS LOGISTICS

IHR PARTNER FÜR DATENSCHUTZGERECHTE AKTENVERNICHTUNG
OB AKTENORDNER, CDS, MIKROFICHE ODER MAGNETBANDSPEICHER...

...nach Ablauf der Aufbewahrungsfristen müssen Datenträger sicher entsorgt werden. Vertrauen Sie auf das Leistungspotenzial und Know-How eines seit vielen Jahren führenden Dienstleisters in der Dokumentenlogistik.

- MOBILE UND STATIONÄRE AKTEN- UND DATENTRÄGERVERNICHTUNG
- OFFICE-ENTSORGUNG
- DATENSCHUTZBERATUNG
- DOKUMENTENTRANSPORTE
- AKTENRETTUNG
- RÜCKNAHMELOGISTIK

Erfahren Sie mehr über uns und unsere Dienstleistungen auf www.aktenvernichtung.de

Rhenus Data Office GmbH · Industriestraße 5 · 48301 Nottuln · Tel.: +49 (0)2509 89-0 · info.data-office@de.rhenus.com · www.aktenvernichtung.de

RECRUITING UNTER DER DSGVO

Nina Diercks

Was hört und liest man nicht alles zur DSGVO im Allgemeinen und zum Thema Recruiting unter der DSGVO im Besonderen. Hartnäckig hält sich etwa das Gerücht, man müsse jeden Bewerber vor der Verarbeitung seiner Daten einwilligen lassen. Insgesamt scheint es so, als sei modernes Recruiting mit der DSGVO nicht mehr möglich. Doch wie so oft lohnt sich auch hier ein nüchterner Blick, um zu erkennen, dass es bei weitem nicht so kompliziert ist, wie von manchem herbeigeschrieben.

Aber man braucht doch immer eine Einwilligung!

Um das gleich zu Beginn richtig zu stellen: Nein, man braucht nur sehr selten eine Einwilligung. Die Einwilligung ist nämlich nur eine von sechs (!) Erlaubnistatbeständen der DSGVO. Und eine Einwilligung kann ein Betroffener jederzeit widerrufen, ein großer Nachteil. Deswegen sollte, wann immer möglich, eine Datenverarbeitung auf einen der anderen fünf Erlaubnistatbestände des Artikel 6 Abs. 1 DSGVO gestützt werden.

§ 26 BDSG – die Rechtsgrundlage zur Verarbeitung von Beschäftigtendaten

Für die Verarbeitung von Daten im Beschäftigtenverhältnis haben wir in Deutschland mit § 26 BDSG (i.V.m. Art. 6 Ib), 88 DSGVO) sogar eine ganz spezielle Norm. In § 26 I BDSG heißt es:

Danach dürfen „personenbezogene Daten von Beschäftigten […] für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung […] erforderlich ist."

Dies bedeutet also, dass all die personenbezogenen Daten von Beschäftigten, die zur Durchführung eines Arbeitsverhältnisses wie etwa Namen, Kontodaten usw. notwendig sind, selbstverständlich durch den Arbeitgeber verarbeitet werden dürfen. Das gilt übrigens auch für sensible Daten wie die Religionszugehörigkeit oder Gesundheitsdaten. Denn auch solche sind natürlich erforderlich, um etwa die Lohnabrechnung ordnungsgemäß vorzunehmen oder eine betriebliche Wiedereingliederungsmaßnahme vorzubereiten und durchzuführen. Dies ergibt sich konkret aus § 26 III BDSG, wonach die Verarbeitung von sensiblen Beschäftigtendaten dann möglich ist, wenn „*sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt*".

Doch zurück zu der Frage, ob ein Unternehmen nicht der Einwilligung zur Verarbeitung von Bewerbern bedürfte. Nein, das ist nicht der Fall. Denn gemäß § 26 VIII 2 BDSG sind: „*Beschäftigte in diesem Sinne […] auch Bewerberinnen und Bewerber*". Da Bewerbungsunterlagen erforderlich sind, um ein Beschäftigtenverhältnis zu begründen, sind natürlich auch Bewerber von der Norm umfasst.

Anders ausgedrückt: Kein Bewerber muss irgendein Einwilligungshäkchen im Online-Karriere-Portal setzen oder seine explizite Zustimmung mit seiner Bewerbung mitschicken. Der potentielle Arbeitgeber ist schlicht aufgrund von § 26 I BDSG zur Verarbeitung der Bewerberdaten berechtigt.

Eine Einwilligung muss nur in einem einzigen Fall eingeholt werden. Und zwar dann, wenn der Bewerber in den unternehmenseigenen Talentpool aufgenommen werden soll. Etwa weil er zwar hochqualifiziert ist, aber ihm derzeit keine Stelle angeboten werden kann. ▸

Sourcing

Doch was tun, wenn man als Unternehmen keine oder keine passenden Bewerbungen mehr erhält? Dann muss ein Unternehmen selbst geeignete Kandidaten suchen, finden und ansprechen. Hier stellt sich nun die Frage, ob Datenverarbeitungen im Rahmen des Sourcings erlaubt sind.

§ 26 BDSG scheidet als Rechtsgrundlage aus. Denn Kandidaten sind – anders als Bewerber – eben keine Beschäftigten im Sinne der Norm. Dies aus gutem Grund: Es besteht noch kein (Vertrauens-) Verhältnis zwischen Kandidaten und Unternehmen. In dem Moment, in dem das Unternehmen einen Kandidaten als potentiell Beschäftigten identifiziert und dessen Daten verarbeitet, weiß der Betroffene schließlich noch nicht einmal davon.

Die gute Nachricht vorab: Auch das Sourcing ist grundsätzlich datenschutzrechtlich zulässig.

Die Bildung eines Talentpools

Die Verarbeitung von Kandidatendaten im Sinne der Bildung eines ersten Talentpools ist auf Art. 6 I f) i.V.m. Art. 9 II e) DSGVO zu stützen. Die Verarbeitung von Kandidatendaten ist demnach dann zulässig, wenn

- ein berechtigtes Interesse des Arbeitgebers vorliegt,
- dem kein überwiegendes Interesse des Kandidaten entgegensteht und
- der Kandidat selbst die verarbeiteten Daten offensichtlich öffentlich gemacht hat.

Dies ist beispielweise ein für jedermann einsehbares Profil in den sozialen Netzwerken.

Dass die Verarbeitung dann erlaubt ist, ergibt sich aus einem Erst-Recht-Schluss: Wenn schon die Verarbeitung besonders schutzwürdiger (sensibler) personenbezogener Daten im Sinne des Art. 9 I DSGVO zulässig ist, wenn der Betroffene sie im Sinne von Art. 9 I e) DSGVO offensichtlich öffentlich gemacht hat, so muss dies erst recht zulässig sein, wenn die Verarbeitung nicht einmal sensible Daten betrifft.

Ein berechtigtes Interesse besteht in der Regel auf Seiten des Arbeitgebers. Ein schlichtes Personalgewinnungsinteresse reicht nämlich aus. Ein entgegenstehendes Interesse des Betroffenen gilt schon deshalb nicht schwerwiegend, weil er die Daten selbst öffentlich machte.

Die Anlage eines Kandidatenpools im Rahmen des Sourcings ist damit zunächst unter Art. 6 I f) iVm 9 II e) DSGVO zulässig.

Die Kandidatenansprache

Mit der Bildung eines Talentpools allein ist jedoch noch nichts gewonnen. Denn die Kandidaten müssen schließlich auch angesprochen werden, um sie als künftige Mitarbeiter gewinnen zu können. Während dies datenschutzrechtlich insoweit unproblematisch ist, da der Verarbeitungsbegriff nach Art. 4 Nr. 2 DSGVO auch das „Nutzen" der Daten umfasst und die Ansprache eine Form der Nutzung darstellt, ist die Ansprache jedoch auch wettbewerbsrechtlich nach dem Gesetz gegen den unlauteren Wettbewerb (UWG) zu betrachten.

Wettbewerbsrecht? Ja, Wettbewerbsrecht. Im Rahmen der Auswahl der am besten geeigneten Kandidaten befinden sich die suchenden Unternehmen in einem Wettbewerb um Personal. Weiter ist die Ansprache von Kandidaten zu Personalgewinnungszwecken gemäß der Definition nach der Art. 2 a) UGP-Richtlinie (RL 2006/114/EG) als Werbung zu verstehen.

Zwar ist die Ansprache von Arbeitnehmern anderer Unternehmen, also das Abwerben, grundsätzlich erlaubt, dies jedoch nur nach bestimmten Regeln.

Die werbliche Direktansprache wird von § 7 UWG geregelt. Demnach wäre die Ansprache per Brief unproblematisch möglich. Ebenso kann der Kandidat telefonisch kontaktiert werden, so lange sich das werbende Unternehmen hier kurzfasst, sachlich bleibt und sich nicht aufdringlich, belästigend oder bedrängend verhält.

Doch ausgerechnet bei elektronischen Nachrichten indes – also bei E-Mails, aber eben auch bei Direct Messages innerhalb von sozialen Netzwerken – sieht § 7 II Nr. 3 UWG vor, dass eine vorherige ausdrückliche Einwilligung des Adressaten vorliegen muss. Diese im Jahr 2019 merkwürdig anmutende Vorschrift macht bei rechtstreuer

Anwendung die elektronische Direktansprache unmöglich.

In der Praxis werden Kandidaten natürlich dennoch kontaktiert. Hier sollte sodann schnellstmöglich eine Einwilligung für die weitere elektronische Kommunikation eingeholt werden. Die möglichen Kosten einer wettbewerbsrechtlichen Abmahnung stehen nämlich gegenüber dem Nutzen des Sourcings in einem sehr vertretbaren Verhältnis. Der Verfasserin sind auch (noch) keine Fälle bekannt, in denen Unternehmen wegen diesbezüglicher unzulässiger E-Mail-Werbung (für einen Job) abgemahnt wurden. Für etwaige Kosten für eine Abmahnung sollte dennoch eine Rückstellung gebildet werden.

Information ist Pflicht

In jedem Fall müssen aber die Informationspflichten nach Art. 12, 13, 14 DSGVO berücksichtigt werden. Der Verantwortliche, hier also der potentielle Arbeitgeber, muss den Bewerber und die Kandidaten nach den gesetzlichen Vorgaben über die Datenverarbeitung informieren, das heißt "Informationen zur Datenverarbeitung", besser bekannt als „Datenschutzerklärung", zur Verfügung stellen. „Informieren" bedeutet jedoch eben nur das ergo zur Kenntnis bringen, nicht jedoch, dass eine „Einwilligung" oder „Zustimmung" einzuholen wäre. Es bedarf auch keiner Check-Box, um sicherzustellen, dass der Bewerber die Datenschutzerklärung gelesen hat. Der Arbeitgeber muss also nur die Kenntnisnahme ermöglichen, nicht aber die tatsächliche Kenntniserlangung sicherstellen.

Fazit

Das Recruiting wird unter der DSGVO an sich nicht komplexer oder unbequemer als zuvor. Die Recruitingprozesse sollten nur einmal ordentlich aufgestellt werden. Was das im Einzelnen bedeutet, können Interessierte nachlesen in dem Fachbeiträgen

Datenschutz im Beschäftigtenverhältnis – Teil 1 - Zeit, mit den Mythen aufzuräumen und endlich das Notwendige zu tun! zfm – Zeitschrift für das Forderungsmanagement Nr. 3/2019, S. 97-104.

Datenschutz im Beschäftigungsverhältnis – Teil 2 – Zeit, mit den Mythen aufzuräumen und endlich das Notwendige zu tun! – zfm - Zeitschrift für das Forderungsmanagement, Nr. 05/2019, S. 186-194.

Über die Autorin

Nina Diercks
Rechtsanwältin (M.Litt, University of Aberdeen) ist seit 2010 ausschließlich im Bereich des IT-, Datenschutz- und Arbeitsrecht tätig. Ebenso so lang schreibt sie zu diesen Themen auf ihrem Blog Diercks Digital Recht. Regelmäßig veröffentlicht sie Fachbeiträge und steht gern und oft als Referentin auf der Bühne. Ab 2020 wird die 39-Jährige als Partnerin zur Hamburger Sozietät Möhrle Happ Luther wechseln und dort den Bereich IT- und Datenschutzrecht verantworten.

▶ www.anwaltskanzlei-diercks.de

ANWALTSKANZLEI DIERCKS

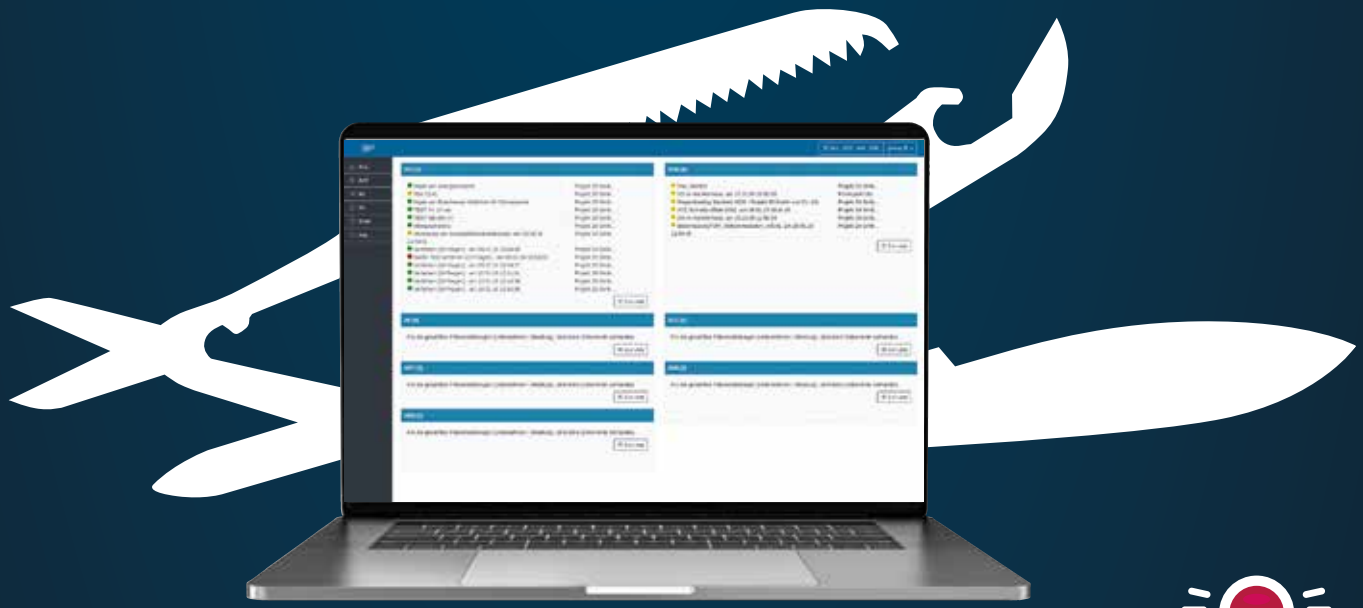
Anzeige

29

PRIVACYSOFT

Die modulare Software-Plattform für alle Aufgaben im Datenschutzmanagement.

PRIVACYSOFT ist eine Marke von Projekt 29 GmbH & Co. KG



DAS DSB-MULTI-TOOL FÜR DIE DATENSCHUTZ BAUSTELLE

KOMPLETTE Datenschutzdokumentation

EXTRA Vorlagen und Checklisten

NEUES Auditmodul

BEWÄHRTE Online-Schulungen

DE/EN/FR Mehrsprachig

INNOVATIONSPREIS-IT BEST OF 2018 initiative mittelstand IT-SECURITY

Software Bundesverband IT-Mittelstand Made in Germany 100% Service Qualität Zukunft

Software Hosted in Germany Bundesverband IT-Mittelstand e.V.

bevh PREFERRED BUSINESS PARTNER

BvD e.V. MITGLIED DATENSCHUTZ GESTALTEN

Projekt 29 GmbH & Co. KG | Ostengasse 14 | 93047 Regensburg | www.privacysoft.de

LÖSCHREGELN FÜR ISSUE-TRACKING-SYSTEME ENTWICKELN

Ein Diskussionsbeitrag zur möglichen Lösung für Löschkonzepte

Annika Selzer, Sarah Stummer

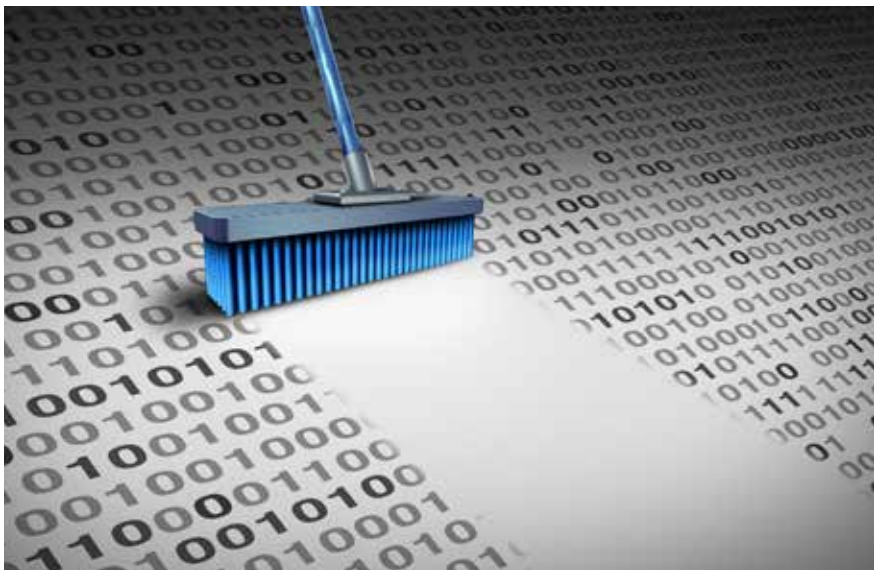
1. Problemstellung[1]

Die Umsetzung datenschutzrechtlicher Löschanforderungen stellt Verantwortliche häufig vor große Schwierigkeiten. Insbesondere in komplexen Datenverarbeitungssystemen, in denen personenbezogene Daten nicht oder nur zum Teil strukturiert vorliegen und deren (voll)automatisches Löschen nicht umgesetzt werden kann, ist die Umsetzung des datenschutzkonformen Löschens mit großen Herausforderungen verbunden. Häufig wird das Begegnen dieser Herausforderungen zusätzlich dadurch erschwert, dass in einem Unternehmen gleich mehrere solcher komplexen Systeme in Benutzung sind – so nutzt beispielsweise nahezu jedes Unternehmen mindestens eine E-Mail-Anwendung, ein CRM-System und ein Issue-Tracking-System (auch als „Ticketsystem" bekannt). Zudem müssen für die Umsetzung des datenschutzkonformen Löschens auch die speziellen technischen und organisatorischen Gegebenheiten der individuellen Systeme berücksichtigt werden.

Um den Verantwortlichen bei der Umsetzung der rechtlichen Vorgaben zu unterstützen, müssen im ersten Schritt pragmatische Löschregeln gefunden werden, die für den jeweiligen Verarbeitungskontext angemessen sind. Dieser Beitrag stellt eine mögliche Lösung für Issue-Tracking-Systeme zur Diskussion.

2. Löschen gemäß Datenschutz-Grundverordnung

Das Löschen personenbezogener Daten wird zunächst durch das Betroffenenrecht auf Löschen aus Art. 17 DSGVO normiert. Es ermöglicht betroffenen Personen unter bestimmten Voraussetzungen zu verlangen, dass der Verantwortliche sie betreffende personenbezogene Daten löscht, etwa wenn ein Widerruf der Einwilligung



vorliegt. Einem Löschbegehren muss jedoch nur entsprochen werden, sofern dem Löschen keine Ausnahmen entgegenstehen. Solche können sich unter anderem aus Art. 17 III DSGVO ergeben und vorliegen, wenn die Verarbeitung zur Erfüllung rechtlicher Verpflichtungen, etwa gesetzlicher Aufbewahrungspflichten erforderlich ist. Gesetzliche Aufbewahrungspflichten können sich unter anderem aus dem Handels- und Steuerrecht ergeben, beispielsweise für Handelsbriefe und Buchungsbelege. Dementsprechend sind Daten bis zum Ablauf der längsten für sie einschlägigen Aufbewahrungspflicht aufzubewahren.

Daneben normieren die Grundsätze der Verarbeitung aus Art. 5 DSGVO die grundsätzliche Pflicht des Verantwortlichen, personenbezogene Daten zu löschen. Insbesondere ist der Grundsatz der Speicherbegrenzung aus Art. 5 I lit. e DSGVO hervorzuheben, der die Löschpflicht des Verantwortlichen insoweit normiert, *als personenbezogene Daten in einer Form gespeichert werden müssen, die die Identifizierung der betroffenen Personen* ▸

[1] Dieser Beitrag wurde vom Bundesministerium für Bildung und Forschung (BMBF) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit unterstützt. Er entstand in Zusammenarbeit mit der Informationssicherheits- und Datenschutzkoordination der Fraunhofer Gesellschaft – die Autoren danken Dr. Ulrich Pordesch für die wertvollen Diskussionen zum Thema.

nur so lange ermöglicht, wie es für die Verarbeitungszwecke erforderlich ist. Insofern trifft den Verantwortlichen die Pflicht, Löschfristen festzulegen, die die Speicherdauer auf das Mindestmaß beschränken.[2]

Korrespondierend zur Löschpflicht obliegt es dem Verantwortlichen nach Art. 5 II, 24 I DSGVO zu dokumentieren und nachzuweisen, dass er seinen datenschutzrechtlichen Pflichten nachkommt.

3. Löschkonzept als organisatorische Maßnahme

Um der Lösch- sowie der Dokumentations- und Nachweispflicht zu entsprechen ist ein datenschutzkonformes Löschkonzept zu erstellen. Ein Löschkonzept definiert vor der Verarbeitung Löschregeln für die zu verarbeitenden personenbezogenen Daten und stellt eine organisatorische Maßnahme dar.

Angemessenheit der Maßnahme

Zu beachten ist, dass solche organisatorischen Maßnahmen angemessen umzusetzen sind. Hierfür ist unter Berücksichtigung der Eintrittswahrscheinlichkeit und der Schwere identifizierter Risiken zu beurteilen, ob eine Verarbeitung ein Risiko oder ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen birgt.

Je wahrscheinlicher der Eintritt der identifizierten Risiken und je schwerer die möglichen Schäden und Folgeschäden, desto höher die Anforderungen an die Maßnahmen. Die Eintrittswahrscheinlichkeit und Schwere des Schadens können jeweils geringfügig, überschaubar, substantiell oder groß sein und sind unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung zu bewerten. Aus der Bewertung der Schadensschwere (geringfügig bis groß) und der Eintrittswahrscheinlichkeit des Schadens (geringfügig bis groß) leitet sich ein geringes, normales oder hohes Risiko ab. So stellt beispielsweise ein geringfügiger Schaden bei einer geringfügigen Eintrittswahrscheinlichkeit ein geringes Risiko dar, während ein großer Schaden mit einer substantiellen Eintrittswahrscheinlichkeit ein hohes Risiko darstellt.[3]

Des Weiteren darf der Verantwortliche die Implementierungskosten berücksichtigen, wodurch ein angemessenes Verhältnis zwischen Kosten und Nutzen hergestellt werden soll. Zudem hat er bei der Festlegung geeigneter Maßnahmen den Stand der Technik zu berücksichtigen.

Orientierung an der DIN 66398

Eine Vorgehensweise zur Entwicklung von Löschregeln beschreibt die DIN 66398, deren Anwendung u.a. von Aufsichtsbehörden empfohlen wird.[4] Die DIN 66398 sieht vor, dass der Datenbestand eines Unternehmens unter Berücksichtigung unter anderem von Rechtsvorschriften (Rechtsgrundlage und Aufbewahrungspflichten), Verwendungszwecken sowie Sensibilität der Daten in sogenannte Datenarten unterteilt wird. Für Datenarten werden zunächst technikunabhängige Löschregeln, bestehend aus Löschfrist und deren Startzeitpunkt, definiert. Anschließend werden prozessspezifische Umsetzungsvorgaben beschrieben.

Maßgeblich für die Löschfrist ist die sogenannte Vorhaltefrist, welche den Zeitraum bildet, in dem die Datenart aufgrund fachlicher Verwendung oder gesetzlicher Aufbewahrungspflichten mindestens benötigt wird.

An die Vorhaltefrist folgt die datenschutzrechtlich vertretbare Frist, innerhalb derer das Löschen der Datenart vorgenommen werden muss. Zusammen ergeben Vorhaltefrist und datenschutzrechtlich vertretbare Frist die Regellöschfrist als maximalen Zeitraum, in dem die Datenart aufbewahrt werden darf (Abbildung 1).

4. Umsetzung von Löschpflichten in Issue-Tracking-Systemen

Wie in der Problemstellung erwähnt kann die Umsetzung datenschutzrechtlicher Löschvorgaben insbesondere in komplexen Datenverarbeitungssystemen wie Issue-Tracking-Systemen mit großen Herausforderungen verbunden sein. Der folgende Abschnitt stellt daher einen Diskussionsbeitrag zur Findung einer pragmatischen Lösung für Issue-Tracking-Systeme dar.

Für die nachfolgend vorgenommene *beispielhafte* Entwicklung von Löschregeln ist zu betonen, dass diese nicht für jedes Issue-Tracking-System ohne weitere rechtliche Prüfung übernommen

[2] Erwgr. 39 DSGVO; Kühling/Buchner/Herbst, DSGVO-Kommentar, Art. 5 DSGVO Rn. 64 f.

[3] DSK, Kurzpapier Nr. 18, S. 5.

[4] Aufsichtsbehörden Hessen/Mecklenburg-Vorpommern/Sachsen/Schleswig-Holstein/der Evangelischen Kirche Deutschland, SDM Baustein 60, S. 5.

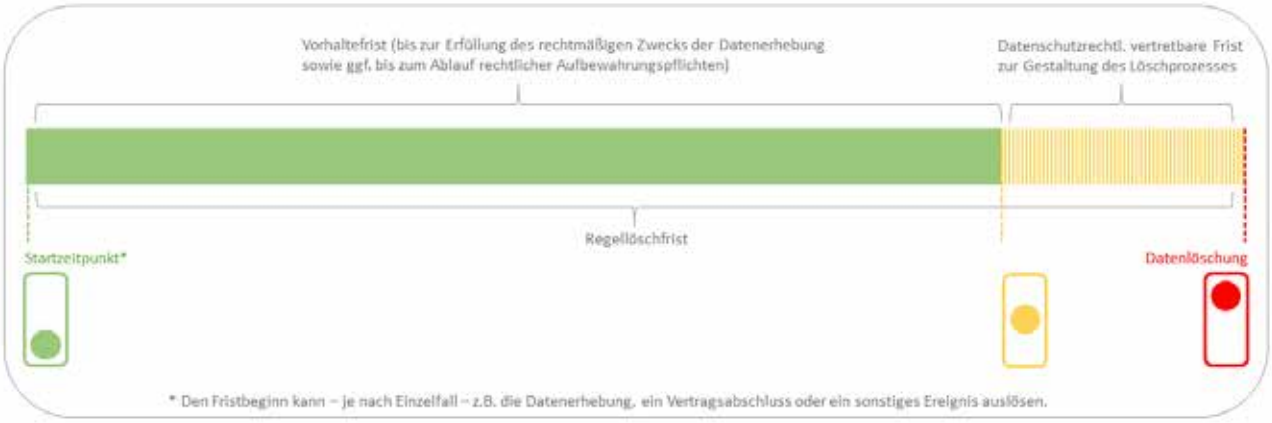


Abbildung 1: Ermittlung der Regellöschfrist einer Datenart [5]

werden können. Eine individuelle Prüfung der Systeme, Rechtsgrundlagen, Verarbeitungszwecke und Zeiträume zur Zweckerreichung ist unbedingt erforderlich.

Überblick über Issue-Tracking-Systeme

Mit Hilfe von Issue-Tracking-Systemen werden in der Regel Anfragen und Probleme von Kunden oder Mitarbeitern systematisch erfasst, kategorisiert, bearbeitet und dokumentiert. Solche Meldungen gehen zum Beispiel über ein Onlineformular ein. Im Hintergrund werden die einzelnen Tickets Sachbearbeitern zur Bearbeitung zugewiesen, die den Bearbeitungsstand aktualisieren und das Ticket nach dessen Bearbeitung „schließen".

Zu jedem Ticket werden strukturierte personenbezogene Daten verarbeitet. Hierzu gehören unter anderem der Vor- und Nachname sowie die Kontaktinformationen des Anfragenden, die vom System über Eingabefelder erfragt werden („Name:____;" „E-Mail-Adresse:_____" usw.).

Darüber hinaus können Tickets eine ganze Reihe unstrukturierter personenbezogener Daten enthalten, die vom Anfragenden als Freitext eingegeben werden („Ihr Anliegen:____"), wie

- Mitarbeiter A meldet den Bedarf eines behindertengerechten Umbaus des Arbeitsplatzes für Mitarbeiterin B. Die Beschreibung des Tickets enthält Informationen zum Gesundheitszustand der Mitarbeiterin B, womöglich eine genaue Diagnose.
- Mitarbeiterin C beantragt Zugriffsrechte auf ein System für den neuen Mitarbeiter D.

Tickets können zudem in ihren Anhängen personenbezogene Daten enthalten, wie Fotos von Personen, fehlerhafte Gehaltsabrechnungen oder buchhaltungsrelevante Unterlagen.

Dementsprechend können Tickets in Freitexten oder Anhängen unstrukturierte personenbezogene Daten enthalten, die sich im Vorfeld nicht kategorisieren lassen. Dazu zählen auch sensible Daten wie Krankheitsdiagnosen.

Zwecke der Datenverarbeitung

Die Datenerhebung dient in der Regel der Bearbeitung von Kundenanfragen und -problemen oder der Aufrechterhaltung der IT- und non-IT-Services bei Mitarbeitern. Nach Bearbeitungsschluss der Tickets können die Daten zusätzlich Rückfragen zu einem Ticket, Berichtszwecken, der Nachvollziehbarkeit von Prozessen und Beteiligten, insbesondere im Fall von IT-Missbräuchen oder Auffälligkeiten, sowie der Wissenssammlung („gab es Problem X schon in der Vergangenheit? Wie wurde es behoben?") dienen. Zudem dient die Erhebung und Weiterverarbeitung von Tickets zur Berechtigungsverwaltung der Erfüllung von Nachweispflichten aus den GoBD[6] sowie dem Datenschutzrecht. Der Beitrag unterstellt das Vorliegen entsprechender Rechtsgrundlagen zur (Weiter)verarbeitung zu den genannten Zwecken.

Zudem unterstellt er, dass die strukturierten personenbezogenen Daten der Anfragenden und der unstrukturierte Personenbezug in Freitextfeldern und Anhängen für die Zwecke, Rückfragen zu beantworten, Prozesse und Beteiligte nachzuvollziehen sowie den Nachweispflichten ▸

[5] Es handelt sich um eine stark vereinfachte Darstellung. Für mehr Details siehe https://www.secorvo.de/publikationen/din-leitlinie-loeschkonzept-hammer-schuler-2012.pdf, S. 15.

[6] GoBD = Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff.

nachzukommen, erforderlich ist, für Berichtszwecke und zur Wissenssammlung jedoch in der Regel nicht.

Die Bearbeitung von Kundenanfragen und -problemen bzw. die Aufrechterhaltung der IT- und non-IT-Services bei Mitarbeitern ist in der Regel mit Abschluss der Ticketbearbeitung erreicht. Mit Rückfragen zu einem geschlossenen Ticket ist mit bis zu sechs Monaten nach Abschluss der Ticketbearbeitung zu rechnen. Die Erreichung der Berichtszwecke ist zwar grundsätzlich von den unternehmensinternen Prozessen abhängig, es wird jedoch davon ausgegangen, dass am Ende eines jeden Jahres Jahresberichte über alle im vorangegangenen Jahr bearbeiteten Tickets erstellt werden und hierfür rund ein Quartal des folgenden Jahres erforderlich ist. Da Auffälligkeiten und IT-Missbräuche in der Regel innerhalb von sechs Monaten auffallen sollten, wird für die Erreichung dieses Zwecks von sechs Monaten nach Schließen des jeweiligen Tickets ausgegangen. Für die Wissenssammlung wird unterstellt, dass Informationen aus Tickets, die älter als drei Jahre sind, nicht mehr relevant sind.

Die Erreichung des Zwecks „Nachweispflichten aus den GoBD" richtet sich nach den Aufbewahrungsfristen der Unterlagen, zu deren Verständnis die GoBD-relevanten Tickets zur Berechtigungsverwaltung erforderlich sind. Die Aufbewahrungsfristen dieser Unterlagen liegen bei bis zu zehn Jahren nach Ablauf des Kalenderjahres, in dem das Dokument entstand, die letzte Eintragung vorgenommen oder die Rechnung ausgestellt oder empfangen wurde (vergl. §§ 147 AO, 258 HGB), weshalb dieser Zweck zehn Jahre nach Ende des Jahres, in dem das Ticket bearbeitet wurde, erreicht ist. Der Zweck der Erfüllung von Nachweispflichten aus dem Datenschutzrecht ist erreicht, sobald die Tickets zur Berechtigungsverwaltung überprüft und die Einhaltung des Berechtigungskonzepts sichergestellt wurden. Jedoch sollte Verantwortlichen nicht das Privileg eingeräumt werden, Tickets zur Berechtigungsverwaltung nie zu überprüfen und diese somit endlos aufzubewahren. Vielmehr sollte ihnen lediglich die Möglichkeit eingeräumt werden ihre Datenschutz-Compliance regelmäßig zu prüfen. Machen sie von dieser Möglichkeit nicht gebrauch, sollten die nicht GoBD-relevanten Tickets zur Berechtigungsverwaltung dennoch nicht länger als drei Jahre aufbewahrt werden.

Angemessenheit von Löschregeln für Issue-Tracking-Systeme

Bei der Entwicklung von Löschregeln sind die Kriterien zur Bestimmung der Angemessenheit technischer und organisatorischer Maßnahmen zu berücksichtigen.

Für die in diesem Beitrag beschriebene Nutzung von Issue-Tracking-Systemen bestehen für die betroffenen Personen insbesondere dann Risiken, wenn diese gegenüber bestimmten Empfängern nicht offenlegen möchten, wo sie wohnen oder arbeiten, dies aber z.B. durch einen IT-Sicherheitsvorfall bekannt werden würde. Verstärkt wird dies, wenn die personenbezogenen Daten nicht von der betroffenen Person selbst zur Verfügung gestellt werden. Zudem können Tickets in Anhängen oder Freitextfeldern sensible personenbezogene oder vertrauliche Daten beinhalten, die aufgrund weiteren denkbaren Risiken einem höheren Schutz bedürfen.

Die Schadensschwere der Risiken ist einzelfallabhängig und kann von leichten bis zu schweren Schäden reichen. Deren Eintrittswahrscheinlichkeit ergibt sich jedoch höchstens indirekt aus der Aufbewahrungsdauer der Daten, wohingegen die zu treffenden technischen und organisatorischen Schutzmaßnahmen – z.B. die verschlüsselte Ablage der Daten und ein strenges, technisch erzwungenes Zugriffsberechtigungskonzept zum Schutz vor unberechtigtem Zugriff auf die Daten – einen direkten Einfluss auf die Eintrittswahrscheinlichkeit haben. Daher ist die Eintrittswahrscheinlichkeit der Risiken für die betroffenen Personen – bei ausreichenden Schutzmaßnahmen – als gering zu bewerten und die Verarbeitung birgt meist ein geringes, allenfalls ein normales Risiko für die betroffenen Personen.

Für die weiteren bei der Angemessenheitsprüfung zu berücksichtigen Faktoren ist festzustellen, dass die Implementierungskosten zur Umsetzung des Löschens grundsätzlich keine Grundlage bilden, um das Löschen zu unterlassen. Es kann jedoch auf ein manuelles Löschen in einem festgelegten Zyklus zurückgegriffen werden, sollten die Implementierungskosten eines automatisierten Löschens außer Verhältnis zum Nutzen stehen. Aufgrund entsprechender Empfehlungen,

insbesondere auch von Aufsichtsbehörden, wird vertreten, dass sich die Entwicklung der Löschregeln an der DIN 66398 als „Stand der Technik" orientieren kann.

Die DIN 66398 empfiehlt bei der Bestimmung von Datenarten die Berücksichtigung der anwendbaren Rechtsvorschriften, der Verarbeitungszwecke, der Kategorien betroffener Personen und der Sensibilität der Daten. Im dargestellten Verarbeitungskontext sind in der Regel sämtliche eingegebene Daten gleichermaßen zur Erreichung der Verarbeitungszwecke erforderlich, unabhängig davon ob sie sensibel sind oder nicht. Zudem ergab die Angemessenheitsprüfung, dass die Verarbeitung sensibler personenbezogener oder vertraulicher Daten kaum höhere Risiken für die betroffenen Personen birgt und diesen Risiken durch weitere technische und organisatorische Maßnahmen entgegengewirkt werden kann.[7]

Für den dargestellten Verarbeitungskontext ergibt sich daher aus Sicht der Autoren eine Angemessenheit für die Unterscheidung nachfolgend dargestellter Datenarten, die zwar die anwendbaren Rechtsvorschriften und Verarbeitungszwecke, nicht aber die Kategorien betroffener Personen und die Sensibilität der Daten berücksichtigt.

Datenarten und deren Löschregeln

Für eine wie in diesem Beitrag genannte Verwendung eines Ticketsystems scheint die Untergliederung in folgende vier Datenarten zur Umsetzung der datenschutzrechtlichen Löschpflichten als angemessen:

- Tickets zu Störungen, Problemen und Änderungen (Datenart A),
- Tickets mit Anträgen und Genehmigungen zur Berechtigungsverwaltung (Datenart B),
- Tickets mit Anträgen und Genehmigungen zur Berechtigungsverwaltung von Datenverarbeitungssystemen (Datenart C) und
- Tickets mit Buchhaltungsdaten (Datenart D).

Die Datenart A umfasst sämtliche Tickets, die keine Berechtigungsverwaltung zum Gegenstand haben. Diese sollten drei Jahre (Löschfrist) nach Ende des Monats, in dem die Tickets geschlossen wurden (Startzeitpunkt), gelöscht oder vollständig anonymisiert werden. Die dreijährige Frist

ergibt sich aus dem Erreichen des Zwecks der Wissenssammlung (Vorhaltefrist). Die Zeit zwischen Ablauf der Vorhaltefrist und Löschen ist die datenschutzrechtlich vertretbare Frist. Zum Schutz der betroffenen Personen sollte mindestens bei den strukturierten Daten (wie Name und E-Mail-Adresse) der Personenbezug bereits sechs Monate nach Ende des Jahres, in dem die Tickets geschlossen wurden, gelöscht beziehungsweise anonymisiert werden.

Dieser Zeitraum basiert auf der Erreichung der Zwecke Rückfragen zu beantworten, Prozesse und Beteiligte nachzuvollziehen sowie Berichte zu erbringen. Zudem wird im Sinne der Angemessenheit der Löschregel aufgrund des erhöhten Schutzbedarfs sensibler personenbezogener sowie vertraulicher Daten empfohlen, den auf Tickets mit solchen Daten zugriffsberechtigten Personenkreis weiter einzuschränken.

Die Datenart B enthält Tickets zur Berechtigungsverwaltung, die nicht GoBD-relevant sind. Sie sollte nach abgeschlossener Überprüfung der Berechtigungsverwaltung, spätestens jedoch drei Jahre (Löschfrist) nach Ende des Monats, in dem die Berechtigung erteilt, geändert oder entzogen wurde, (Startzeitpunkt) gelöscht werden.

Die Löschregel basiert auf der Erfüllung datenschutzrechtlicher Nachwespflichten (Vorhaltefrist). Die Zeit zwischen Ablauf der Vorhaltefrist ▸

[7] Grundsätzlich bedarf jede Entscheidung der angemessenen Umsetzung von Maßnahmen die individuelle Bewertung des Verarbeitungskontextes. Insofern ist für die im jeweiligen Ticketsystem anfallenden personenbezogenen Daten und die Kategorien betroffener Personen eine individuelle Risikobewertung durchzuführen.

und Löschen ist die datenschutzrechtlich vertretbare Frist.

Die Datenart C enthält Tickets zur Berechtigungsverwaltung, die GoBD-relevant sind. Tickets in dieser Datenart sollten zehn Jahre (Löschfrist) nach Ende des Jahres, in dem die Berechtigung erteilt, geändert oder entzogen wurde (Startzeitpunkt), gelöscht werden. Die zehnjährige Frist basiert auf der Erreichung des Zwecks der Erfüllung von Nachweispflichten nach den GoBD (Vorhaltefrist). Da die Datenarten B und C dem Zweck der Wissenssammlung nicht dienen, sollten diese Datenarten sechs Monate nach Ende des Jahres, in dem sie geschlossen wurden, zugriffsbeschränkt archiviert werden. Dieser Zeitraum basiert auf der Erreichung der übrigen Verarbeitungszwecke.

Grundsätzlich sollte für alle Datenarten die Möglichkeit bestehen das Löschen auszusetzen bzw. – soweit aufgrund gesetzlicher Aufbewahrungspflichten zulässig – vorzeitig zu vollziehen. Auszusetzen ist das Löschen etwa, wenn ein Ticket für eine Rechtsstreitigkeit erforderlich ist oder ein rechtmäßiger Sperrantrag nach Art. 18 DSGVO vorliegt. Vorzeitig zu vollziehen ist sie, wenn ein rechtmäßiger Löschantrag nach Art. 17 DSGVO vorliegt.

Sollten Tickets in Ausnahmefällen aufbewahrungspflichtige Unterlagen enthalten, deren Aufbewahrung direkt im Issue-Tracking-System erfolgen muss, sind diese einer anderen Datenart zuzuordnen. Die Löschregeln dieser Datenart(en) richten sich nach den geltenden Aufbewahrungsvorschriften und Verarbeitungszwecken. Ein Beispiel hierfür ist die Datenart D, zu der Buchhaltungsunterlagen zählen, für welche in der Regel zehnjährige Aufbewahrungspflichten bestehen (§§ 147 AO, 257 HGB). In diesem Fall gilt für die Löschregel eine Vorhaltefrist von 10 Jahren und ein Startzeitpunkt zum Schluss des Kalenderjahres, in dem die Buchung getätigt wurde. Aufgrund der Angemessenheit der Maßnahme sollten die Daten spätestens zwei Jahre nach Ende des Jahres, in dem die Buchung getätigt wurde, zugriffsbeschränkt archiviert werden.

5. Fazit

Zur Entwicklung von Löschregeln für Issue-Tracking-Systeme ist eine Orientierung am Prinzip der DIN 66398 hilfreich, wonach „einfache Löschregeln […] der Schlüssel zum Erfolg" sind. Für die hier vorgenommene beispielhafte Entwicklung von Löschregeln bleibt zu betonen, dass diese nicht für jedes Issue-Tracking-System ohne weitere rechtliche Prüfung übernommen werden können. Vielmehr erfordert die Entwicklung datenschutzkonformer Löschregeln eine individuelle Prüfung der Systeme, Rechtsgrundlagen, Verarbeitungszwecke und Zeiträume zur Zweckerreichung.

Weiterhin sind im Rahmen der Dokumentations- und Nachweispflicht zum Löschen konkrete Umsetzungsvorgaben zu entwickeln, die Löschregeln zu implementieren und dies sowie deren Umsetzung zu protokollieren. Zudem sind Handlungsanweisungen für die mit dem Issue-Tracking-System arbeitenden Mitarbeiter bereitzustellen, die anweisen nicht erforderliche personenbezogene Daten zu entfernen. Schließlich sind die Löschregeln auf deren Wirksamkeit und Geeignetheit zu prüfen und gegebenenfalls anzupassen. Erst hierdurch wird das datenschutzkonforme Löschen in Issue-Tracking-Systemen gewährleistet.

Über die Autorinnen

Annika Selzer
arbeitet als Senior Researcher am Fraunhofer SIT in Darmstadt.

Sarah Stummer
ist Mitarbeiterin in der Datenschutzkoordination am Fraunhofer SIT, Darmstadt.

▶ www.sit.fraunhofer.de

Fraunhofer SIT

UNTERAUFTRAGSVERARBEITER WECHSELN? WIE SIE FALLSTRICKE VERMEIDEN

Dr. Niels Lepperhoff

Das Leben als Auftragsverarbeiter ist wahrlich nicht einfach. Da Art. 28 DSGVO die Pflichtinhalte für den Auftragsverarbeitungsvertrag (AVV) im Vergleich zum § 11 BDSG-alt verändert hatte, waren neue Verträge nötig. Auf den ersten Blick wirkte der Austausch der Verträge wie ein rein formaler – ja bürokratischer – Akt. Vielfach drängte sich der Eindruck auf, dass außer den beteiligten DSB auf der Fachseite weder Auftraggeber noch Auftragnehmer am Inhalt sonderlich interessiert waren.

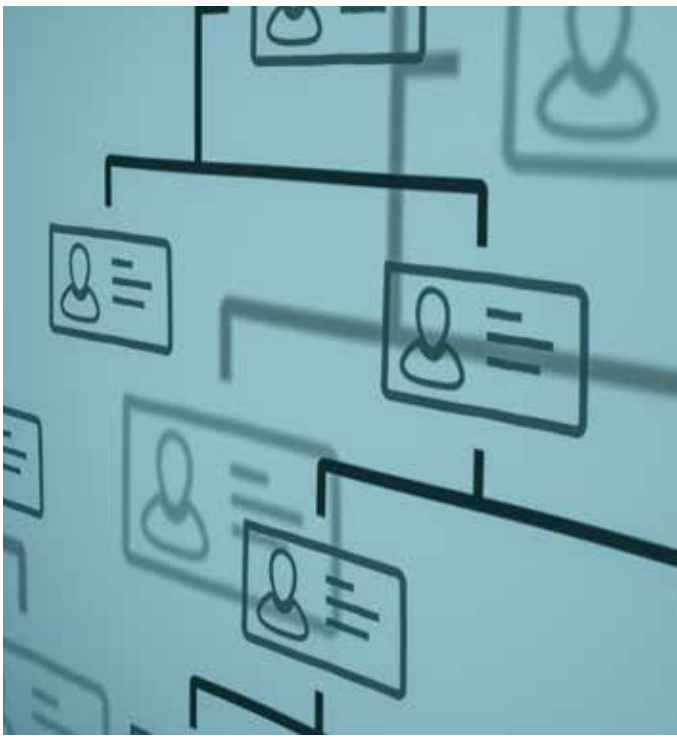
Soll ein Unterauftragsverarbeiter ausgetauscht werden, gewinnt der AVV plötzlich an Bedeutung, da er eine Unterbeauftragung regelt. Jedenfalls sollte man meinen. Der Fall der X GmbH illustriert, welche Fallstricke es zu vermeiden gilt.

Die X GmbH bietet ihr Softwareprogramm als Software as a Service (SaaS) ihren Kunden an. Mit den Kunden wurden AVV geschlossen. Die Software wird bei einem Unterauftragsverarbeiter (UAV), der M GmbH gehostet. Nun soll von der M GmbH zu A plc. gewechselt werden. A plc. ist ein international tätiges Unternehmen, das als Markführer für Hostingleistungen gilt.

Fallstrick Widerspruch vs. Zustimmung

Die X GmbH informierte ihre Kunden über den Wechsel zu A plc. und räumte ein 14-tägiges Widerspruchsrecht ein. Dumm war nur, dass die mit den Kunden geschlossene AVV eine Zustimmung statt eines Widerspruchs vorsah. Für eine verweigerte Zustimmung hatte die X GmbH auch kein Sonderkündigungsrecht vereinbart. Bei verweigerter Zustimmung ist sie deshalb weiter leistungspflichtig.

Im Massengeschäft SaaS ist eine Widerspruchslösung immer einer Zustimmung vorzuziehen. Eine Zustimmung erfordert eine aktive Handlung des Kunden. Unterbleibt diese – gleich aus welchen



Gründen – darf der neue UAV für Kunden ohne erteilte Zustimmung nicht eingesetzt werden. Gleichzeitig besteht Leistungspflicht diesen Kunden gegenüber. Bei der Widerspruchslösung lässt sich durch Fristsetzung der Zeitpunkt festlegen, ab dem für alle Kunden, die keinen Widerspruch ausgesprochen haben, der neue UAV eingesetzt wird. Kunden, die passiv bleiben, wechseln zum neuen UAV. Für die widersprechenden Kunden besteht ebenfalls weiterhin Leistungspflicht, ohne den neuen UAV einsetzen zu dürfen.

Um die Leistungspflicht bei nicht erteilter Zustimmung oder ausgeübtem Widerspruch beenden zu können, sollte ein entsprechendes Kündigungsrecht, das als Kündigungsgrund die nicht erteilte Zustimmung oder den ausgeübten Widerspruch vorsieht, vertraglich vor dem UAV-Wechsel vereinbart werden. ▸

Fallstrick Vertragswahl

Wer es sich durch seine Marktmacht leisten kann, seine eigenen Prozesse vertraglich durchzusetzen, hat es einfach. Er kann bspw. mit einheitlichen Widerspruchsfristen operieren. Alle übrigen Auftragsverarbeiter leben regelmäßig mit einer Mischung aus verschiedenen vertraglichen Vereinbarungen. In der Praxis bietet es sich an, die wesentlichen vereinbarten Fristen und Abläufe standardisiert bspw. im CRM am Kunden zu hinterlegen.

Fallstrick Kontrollrechte

Art. 28 Abs. 3 lit. h) DSGVO verlangt, dass der Auftragsverarbeiter „dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt." Entsprechende Regelungen, d.h. Einräumung von Kontrollrechten vor Ort und Zusicherung einer Unterstützung und Mitwirkung durch den UAV zu Gunsten des Auftragsverarbeiters, sind in der AVV zu treffen.

Je nach Risiko empfiehlt es sich, mit den UAV zusätzlich Kontrollrechte zugunsten des Kunden des Auftragsverarbeiters zu vereinbaren. Wenn die AVV mit den Kunden Regelungen enthalten, die den Auftragsverarbeiter verpflichten, bei seinen UAV Kontrollrechte für die Kunden zu vereinbaren, sind entsprechende Regelungen zwingend mit dem UAV zu treffen.

Im vorliegenden Fall wurde vereinbart, dass die X GmbH neben dem eigenen Kontrollrecht auch ein Kontrollrecht zu Gunsten des Kunden mit den UAV vereinbart. Das ist ungünstig, wenn der ausgewählte UAV A plc. weder der X GmbH noch deren Kunden ein Kontrollrecht einräumt. A plc. verengt das Kontrollrecht auf die Entgegennahme von Prüfberichten der von A plc. bezahlten und beauftragten Prüfer.

Solche Prüfungen können eine Kontrolle durch den Auftragsverarbeiter oder seinen Kunden nicht ersetzen, da die Prüfer weder den Umgang mit Daten dieses konkreten Kunden betrachten, noch dem Auftragsverarbeiter oder seinen Kunden gegenüber ungefiltert Bericht erstatten und diesen verpflichtet sind. Gegenüber ihrem Kunden begründet die X GmbH das fehlende Kontrollrecht sinngemäß mit der hohen Kundenanzahl von A plc. und damit, dass die Standorte der Rechenzentren aus Sicherheitsgründen geheim zu halten seien. Abgesehen davon, dass Art. 28 Abs. 3 lit. h) DSGVO keine Ausnahme kennt, spricht weder eine hohe Kundenanzahl gegen Kontrollen, noch der Versuch, „security by obscurity" zu erreichen.

Wenn die Sicherheit eines Rechenzentrums daran hinge, dass der Standort unbekannt bleiben muss, wären erhebliche Zweifel angebracht, dass dort ein risikoangemessener Schutz nach Art. 32 DSGVO besteht.

Im Übrigen ist der Standort für Mitarbeiter von Energieversorgern einfach in Erfahrung zu bringen. Der Stromverbrauch und die warme Abluft verraten regelmäßig Rechenzentren. Ob die X GmbH diese Aussage mit A plc. abgestimmt hatte, entzieht sich der Kenntnis des Autors.

Fallstrick Zugriffe aus Drittstaaten

A plc. ist ein Unternehmen mit verschiedenen Gesellschaften in Drittstaaten. Aus diesen Gesellschaften kann auf die Daten des Kunden zugegriffen werden. Nicht nur die Speicherung im Drittstaat, sondern bereits ein Zugriff aus einem Drittstaat bedarf der dokumentierten expliziten Weisung des Kunden. Die Weisung muss sich auf den Datenexport in den entsprechenden Drittstaat beziehen.

Die Erforderlichkeit einer expliziten Weisung ist in der AVV zwingend zu regeln (Art. 28 Abs. 3 lit. a) DSGVO). Um die Zustimmung zu erteilen, benötigt ein Kunde nicht nur die Liste der zugreifenden Unternehmen mit Firmierung und Land des Zugriffs, sondern auch eine Beschreibung der Tätigkeiten sowie eine Angabe, mit welchem Instrument (Angemessenheitsbeschluss, EU-Standardvertrag, BCR) für ein angemessenes Datenschutzniveau gesorgt wird. Eine solche Liste wird ebenfalls für alle Auftragsverarbeiter in der Kette benötigt.

Diese Informationen werden vom Kunden auch für die Aktualisierung der Informationen für Betroffene nach Art. 13 und 14 DSGVO benötigt. Die Informationspflicht ergibt sich daraus, dass der Kunde mit dem UAV gesamtschuldnerisch haftet. In diesen Informationen für Betroffene sind die neuen Empfänger mindestens als Kategorie und Drittstaaten mit den entsprechenden Instrumenten aufzunehmen. Im vorliegenden Fall nannte die X GmbH auch auf explizite Nachfrage weder die Tätigkeiten noch das Instrument zur Sicherstellung eines angemessenen Datenschutzniveaus. Eine Weisung zum Datenexport konnte folglich nicht erteilt werden.

Fallstrick Weitergabe von Pflichten an UAV

Grundsätzlich sehen die Musterverträge zur AV vor, dass der Auftragsverarbeiter seine Pflichten aus dem AVV an den UAV weiterreicht. Auch in dem AVV mit der X GmbH findet sich eine entsprechende Regelung. Da die Kontrollrechte des Kunden nicht an A plc. weitergereicht worden sind, würde die X GmbH bei Beauftragung von A plc. gegen diese Klausel verstoßen.

Bei einer Beauftragung eines UAV ist deshalb genau zu prüfen, welche Pflichten der Auftragsverarbeiter mit seinen Kunden vereinbart hat. Diese Pflichten sind in dem AVV mit dem UAV aufzunehmen. Auftragsverarbeiter, die unterschiedliche AVV mit ihren Kunden abschließen, müssen die unterschiedlichen Regelungen aus allen AVV berücksichtigen.

Fallstrick Geeignete Garantien

Art. 28 Abs. 1 DSGVO verlangt vom Verantwortlichen, nur mit Auftragsverarbeitern zusammenzuarbeiten, „die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet."

Diese Vorgabe gilt auch für Auftragsverarbeiter im Verhältnis zu ihren UAV (Art. 28 Abs. 4 DSGVO). Beauftragt ein Auftragsverarbeiter wie im vorliegenden Fall einen UAV, der keine Kontrollrechte einräumt, so ist offensichtlich, dass der UAV die DSGVO nicht vollumfänglich einhält. Der Auftragsverarbeiter verstößt in der Folge gegen Art. 28 Abs. 4 DSGVO.

Genehmigt der Kunde diesen UAV oder legt er keinen Widerspruch ein, so verstößt er ebenfalls gegen Art. 28 DSGVO, da er einen Auftragsverarbeiter einsetzt, von dem er weiß, dass dieser gegen Vorschriften der DSGVO verstößt.

Fallstrick Kommunikation mit dem Kunden

Steht der Wechsel zum neuen UAV an, muss der Kunde informiert und um Zustimmung gebeten oder auf sein Widerspruchsrecht inkl. Frist hingewiesen werden. Es empfiehlt sich, die Folgen einer nicht erteilten Zustimmung oder eines eingelegten Widerspruchs darzustellen. Damit lassen sich Rückfragen reduzieren.

Fazit

Der geschilderte Fall illustriert eindrücklich, worauf beim Wechsel eines UAV zu achten ist. Er macht auch deutlich, dass ein potenzieller Wechsel schon bei der Gestaltung der Vertragsbeziehung mit den Kunden einzuplanen ist:

- AVV des Kunden vs. AVV des Auftragsverarbeiters
- Zustimmung vs. Widerspruch und
- Folgen bei verweigerter Zustimmung oder ausgeübtem Widerspruchsrecht.

Bei der Auswahl des UAV ist auch darauf zu achten, dass die eigenen Pflichten den Kunden gegenüber vom Auftragsverarbeiter auf den neuen UAV überleitbar sind.

Der Wechsel eines UAV zeigt exemplarisch, wie die Regelungen in der AVV auf das Geschäft und die Beziehungen zu Kunden durchschlagen. Geschäftsführer und Fachabteilungen tun deshalb gut daran, sich intensiver mit den Regelungen im AVV zu befassen.

Erstaunlich ist, wie viele Unternehmen fehlende Kontrollrechte hinnehmen, obwohl das Fehlen ein Bußgeldrisiko von bis zu zehn Millionen Euro oder – sofern höher – zwei Prozent des weltweiten Vorjahresumsatzes des Unternehmensverbundes bedeutet. Ob der nicht spürbare Verfolgungsdruck diese Haltung begünstigt? Für die gesetzestreuen Unternehmen ist die Lethargie in der Verfolgung bedrohlich, da die im Einklang mit Art. 28 DSGVO einsetzbaren Auftragsverarbeiter mit jedem Wechsel zu A plc. als UAV weniger werden. Auch Vertragsstrafen helfen nicht weiter, wenn ein abrupter Wechsel des Auftragsverarbeiters zu spürbaren Störungen in den Leistungen des Kunden führen würde.

Über den Autor

Dr. Niels Lepperhoff

Geschäftsführer der Xamit Bewertungsgesellschaft mbH und der DSZ Datenschutz Zertifizierungsgesellschaft mbH
(einem Gemeinschaftsunternehmen des BvD e.V. und der GDD e.V.).

▶ http://www.xamit-leistungen.de/unternehmen/das-xamit-team.php

ÜBERARBEITETE PRAXISHILFE ZUR DSFA IM GESUNDHEITSWESEN LIEGT VOR

Dr. Bernd Schütze

Eine der größten Herausforderungen, welche die Datenschutz-Grundverordnung (DS-GVO) enthält, stellt sicherlich die Datenschutz-Folgenabschätzung (DSFA) dar. Art. 35 Abs. 3 lit. b DS-GVO stellt fest, dass bei einer „umfangreichen" Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs.1 DS-GVO eine DSFA erforderlich ist.

Für eine Verarbeitung von Gesundheitsdaten wie auch genetische Daten ist somit immer eine DSFA notwendig, wenn das Kriterium „umfangreich" erfüllt ist – was bei Institutionen wie Krankenhäusern oder größeren Forschungsprojekten wie bei multizentrischen klinischen Studien vermutlich erfüllt wird.

Im April 2018 veröffentlichten die Deutsche Krankenhausgesellschaft e.V. (DKG), der Bundesverband Gesundheits-IT e. V. (bvitg) und die Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS) eine Praxishilfe für das Gesundheitswesen, welche Erläuterungen zu Art. 35 DS-GVO, aber auch Hinweise für die praktische Durchführung der DSFA enthält. Bedingt durch den Aufwand, den die DS-GVO bei allen Beteiligten Ende 2017/Anfang 2018 verursachte, konnte zu dem Zeitpunkt noch keine Diskussion mit den Datenschutz-Aufsichtsbehörden durchgeführt werden. Von August 2018 bis August 2019 erfolgte ein reger Austausch mit dem Arbeitskreis „Gesundheit und Soziales" der Datenschutzkonferenz. Der äußerst konstruktive Dialog führte zu einer umfangreichen Überarbeitung der Praxishilfe (und einem deutlich Anstieg der Seitenzahlen). Die Praxishilfe steht nunmehr in der zweiten Version online zur Verfügung[1]. Im Folgenden werden die wichtigsten Änderungen zur Vorgängerversion in aller Kürze vorgestellt.

Grundlegender Aufbau

Die Beispiele für Datenarten, Erlaubnistatbestände und weitere wurden aus dem eigentlichen Text herausgenommen und in einen eigenen Anhang 1 überführt. Dabei wurden natürlich die Angaben noch einmal durchgesehen und überarbeitet. So wurden einige Beispiele für die Erlaubnistatbestände hinsichtlich der deutschen Gesetzgebung weiter konkretisiert.

[1] bvitg, DKG, GMDS: Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO. Online unter https://ds-gvo.gesundheitsdatenschutz.org/html/dsfa.php (Zitiert 2019-10-14)

In einem Anhang 3 wurden alle Erwägungsgründe aufgenommen, die im Text angeführt werden. Jeder Datenschutzbeauftragte wird vermutlich mit dem Text der DS-GVO „unter dem Kopfkissen schlafen" und immer alle Texte griffbereit haben. Aber zu einem DSFA-Team gehören viele Experten, die nicht aus dem Datenschutz-Umfeld kommen. Für diese Personen ist es vermutlich hilfreich, wenn die Texte in der Praxishilfe vorhanden sind und nicht über eine Internet-Suchmaschine gesucht werden müssen.

Natürlich wurde auch das Kapitel mit den Literaturhinweisen aktualisiert. Im Überarbeitungszeitraum sind gerade in den juristischen Fachzeitschriften diverse Artikel zum Thema DSFA erschienen.

Kommentierung des Art. 35 DS-GVO

Alle Abschnitte wurden überarbeitet. Beispielsweise wurde das Kapitel hinsichtlich der Verarbeitung ohne Einwilligung des Betroffenen an die deutsche Gesundheitsgesetzgebung angepasst und im Abschnitt zu den Rechten und Freiheiten natürlicher Personen auf den zu beachtenden europarechtlichen Kontext bei der Auslegung hingewiesen.

Art der Daten

Hinzu kam ein neuer Abschnitt zu den Datenarten. Die DS-GVO unterscheidet ja zwischen „normalen" Daten und Daten der besonderer Kategorien gem. Art. 9 Abs. 1. Hier war wieder der Gedankengang, dass die Praxishilfe das gesamte DSFA-Team adressieren soll, also auch Personen, die nicht aus der Datenschutzpraxis kommen und die für eine Erklärung dankbar sind.

Risiko der Verarbeitung

Die Thematik rund um den Begriff „Risiko" wurde vollständig überarbeitet. Die Definition ist aus den Begrifflichkeiten der DS-GVO abgeleitet. Das Risiko wurde abhängig von der Eintrittswahrscheinlichkeit und der Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen (= „Schadenshöhe") dargestellt. Dies entspricht der „klassischen" Definition eines Risikos, wie es sich in verschiedenen internationalen Normen wiederfindet.

Die Klassifizierung von Risiken wurde an die Begrifflichkeiten der DS-GVO angepasst. Die DS-GVO benutzt an den verschiedenen Stellen Begrifflichkeiten, um den Grad des Risikos darzustellen.

Beispiele hierfür sind „erhebliche Risiken" in Erwägungsgrund 51 oder „kein Risiko" in Erwägungsgrund 80. Die verschiedenen textuellen Vorgaben des europäischen Gesetzgebers wurden zusammengetragen und daraus die nachfolgend dargestellte Abstufung zur Einteilung von Risiken abgeleitet:

- Hohes Risiko
- Erhebliches Risiko
- (Normales) Risiko
- Voraussichtlich kein Risiko
- Kein Risiko

Durchführung einer DSFA

Auf Anregung der Aufsichtsbehörden wurde das Kapitel zur Durchführung einer DSFA um einen Abschnitt hinsichtlich der Identifizierung betroffenen Daten erweitert. Jedem im Datenschutzumfeld Tätigen ist in „Fleisch und Blut" übergegangen, dass immer an erster Stelle geklärt werden muss, um welche personenbezogene Daten es geht. Aber die Praxishilfe soll ja auch eine Orientierung für Personen darstellen, die sich vielleicht erstmals mit dem Thema beschäftigen und daher diese Information brauchen.

Da das Thema „Risiko" bei der rechtlichen Betrachtung überarbeitet wurde, mussten natürlich auch die entsprechenden Abschnitte bei der Durchführung neu gestaltet werden.

Bei der Risikoklassifizierung wurde beispielsweise eine Risikomatrix entsprechend DIN ISO/TR 14121-2 aufgenommen[2], an Hand derer auch optisch ersichtlich wird, welche Risiken akzeptabel sind und welche nicht (wobei die Beurteilung bezüglich der Akzeptanz vom Verantwortlichen selbstverständlich aus Sicht der betroffenen Person heraus getroffen werden muss). Das Kapitel „Umgang mit den datenschutzrechtlichen Risiken" wurde um die Betrachtung des Angreifermodells erweitert. ▸

[2] Risikomatrix entsprechend DIN ISO/TR 14121-2. „Sicherheit von Maschinen - Risikobeurteilung - Teil 2: Praktischer Leitfaden und Verfahrensbeispiele". Deutscher Vertrieb bei Beuth, www.beuth.de/de/technische-regel/din-iso-tr-14121-2/169319397 (Zitiert 14.10.2019)

DSFA-Bericht

Der in der ersten Version der Praxishilfe dargestellte Vorschlag für die strukturierte Dokumentation einer Datenschutz-Folgenabschätzung ist ebenfalls überarbeitet worden. Bei der Darstellung der potenziellen Risiken wurde beispielsweise die Risiko-Identifikationsmatrix als Möglichkeit zur Verdeutlichung des Zusammenhangs zwischen Risikoursachen und Risikoauswirkungen dargestellt.

In der ersten Version war kein Abschnitt für die Risikoanalyse vorgesehen, da wir davon ausgingen, dass jedem offensichtlich ist, dass zu einem DSFA-Bericht natürlich die Risikoanalyse gehört. Die Kolleginnen und Kollegen von den Aufsichtsbehörden merkten zu Recht an, dass dies jedem klar sein mag, aber dass man in einem entsprechenden Vorschlag angeben muss, wo dieser Teil der DSFA abgebildet wird. Entsprechend ist jetzt hierfür ein eigener Abschnitt vorgesehen.

Das Kapitel zur Darstellung der Erbringung der Anforderungen aus Art. 32 DS-GVO wurde ebenfalls aktualisiert. Insbesondere wurden Hinweise zur Dokumentation der Verschlüsselung aufgenommen, da man nicht bei allen, die eine DSFA durchführen, voraussetzen kann, dass sie an die zur Überprüfbarkeit notwendigen Angaben denken.

Next Steps

Basierend auf der Praxishilfe erarbeitet derzeit eine Gruppe eine DSFA für ein fiktives Krankenhausinformationssystem, einerseits um die am grünen Tisch erarbeiteten Empfehlungen hinsichtlich der praktischen Umsetzbarkeit zu überprüfen, andererseits um durch eine Beispiel-DSFA Verantwortlichen einen Hinweis zum Vorgehen und insbesondere für die Aufwandsabschätzung anzubieten. Ein Krankenhausinformationssystem wurde deswegen gewählt, weil die Artikel-29-Datenschutzgruppe in ihrem Papier zur DSFA schrieb, dass für derartige Systeme grundsätzlich eine DSFA erforderlich sei. Dies bedeutet letztlich, dass jedes Krankenhaus eine entsprechende DSFA benötigt und ein entsprechender Bedarf an einem Beispiel vorausgesetzt werden kann.

Als „Nebenergebnis" wollen wir Werkzeuge, mit denen die Bespiel-DSFA erstellt wurde, zur Verfügung stellen. Geplant ist eine Word-Vorlage für den DSFA-Bericht und eine Excel-Tabelle zur Darstellung der Risikoanalyse und Risikobehandlung.

Fazit

Die Praxishilfe ist in erster Linie für Verantwortliche im Gesundheitswesen geschrieben und enthält viele Hinweise, wie beispielsweise Verarbeitungszwecke oder Erlaubnistatbestände aussehen können. Abgesehen von diesen Punkten aus dem Gesundheitsbereich sind die rechtliche Betrachtung des Art. 35 DS-GVO in Kapitel 3, die Darstellung der Vorgaben der Aufsichtsbehörden in Kapitel 4, der Vorschlag bzgl. der Vorgehensweise bei der Erstellung einer Datenschutz-Folgenabschätzung in Kapitel 5 sowie der Vorschlag für die strukturierte Dokumentation einer Datenschutz-Folgenabschätzung in Kapitel 6 allgemein gehalten und nicht speziell auf das Gesundheitswesen angepasst. Die Praxishilfe stellt somit für jeden Verantwortlichen, der sich mit dem Thema DSFA auseinandersetzen muss, nützliche Informationen zur Verfügung.

Danksagung

An dieser Stelle sei allen Personen der Aufsichtsbehörden, die sich an der Kommentierung des Textes beteiligten, noch einmal der herzlichste Dank unserer Arbeitsgruppe ausgesprochen: Wir sind fest davon überzeugt, dass unsere Praxishilfe durch den Dialog und den daraus resultierenden Überarbeitungen deutlich gewonnen hat und die Leser dieser Praxishilfe somit noch mehr Nutzen aus ihr ziehen können.

Über den Autor

Dr. Bernd Schütze

beschäftigt sich seit 1995 mit den datenschutzrechtlichen Aspekten innerhalb der Gesundheitsversorgung. Nach gut dreißigjähriger beruflicher Tätigkeit in verschiedenen Krankenhäusern arbeitet Dr. Schütze seit 2014 als „Senior Experte Medical Data Security" bei der Deutschen Telekom Healthcare and Security Solutions GmbH. Als Lehrbeauftragter ist er zudem an verschiedenen Hochschulen tätig und veröffentlicht regelmäßig Beiträge in Büchern und Fachzeitschriften.

Anzeige

Steckt auch in Ihnen die **Service-DNA**?

Dann verbinden Sie sich jetzt mit dem größten Service-Netzwerk Europas*:

Werden Sie Mitglied im Service-Verband KVD e. V. und profitieren Sie neben dem professionellen Netzwerk mit den Verbindungen in Praxis, Forschung und Politik auch von der internationalen Zusammenarbeit des KVD, zum Beispiel mit dem österreichischen Verband KVA und dem Schweizer Pendant, dem SKDV.

Informieren Sie sich jetzt unter **www.kvd.de**.

* Der KVD gilt mit seinen 1.600 Mitgliedern als größtes verbandliches Service-Netzwerk seiner Art in Europa. Er unterstützt Fach- und Führungskräfte bei der Gestaltung ihres technischen Kundendienstes. Über Netzwerkveranstaltungen, Aus- und Weiterbildungen sowie die Einbindung neuester Forschungsergebnisse erhalten Mitglieder einen entscheidenden Wissens- und damit Marktvorsprung.

DAS ZWEITE DSANPUG-EU UND DIE ÄNDERUNGEN DES BDSG

Dr. Tilman Dralle

I. Einleitung

Nach der grundlegenden Novellierung des deutschen Bundesdatenschutzgesetzes (BDSG) alter Fassung nach Inkrafttreten der EU-Datenschutz-Grundverordnung (DSGVO) im Jahr 2017 hat, nach dem Deutschen Bundestag am 27. Juni 2019, nun auch der Deutsche Bundesrat in seiner Sitzung am 20. September 2019 das Zweite Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU, kurz: 2. DSAnpUG-EU) angenommen. Das 2. DSAnpUG-EU enthält etliche Änderungen des BDSG neuer Fassung sowie zahlreicher bereichsspezifischer Datenschutzregelungen in insgesamt 153 Bundesgesetzen – vom Antiterrordateigesetz bis hin zum Zahlungsdiensteaufsichtsgesetz. Es tritt nach seiner Veröffentlichung im Bundesgesetzblatt voraussichtlich zum Jahresende in Kraft.

Neben rein redaktionellen Anpassungen von Begriffsbestimmungen und Verweisen an die DSGVO werden durch das 2. DSAnpUG-EU auch materiell-rechtlich relevante Änderungen vorgenommen. Dieser Beitrag gibt einen Überblick über sämtliche Neuerungen für privatwirtschaftliche Unternehmen in Bezug auf das BDSG und offeriert jeweils eine prägnante Bewertung aus juristischer und praktischer Sicht (dazu unter II.). Darüber hinaus werden vier Regelungsbereiche beispielhaft betrachtet, in denen der Gesetzgeber ungeachtet entsprechender Entwicklungen eine Änderung respektive Konkretisierung des BDSG versäumt beziehungsweise unterlassen hat (dazu unter III.).

II. Die Änderungen des BDSG

1. Gleichstellung von Nicht-EU-Mitgliedstaaten (§ 1 BDSG)

Gemäß Kapitel V der DSGVO unterliegt jede Übermittlung personenbezogener Daten an ein Drittland besonderen Voraussetzungen. Zwar enthält die DSGVO keine Legaldefinition des Begriffs „Drittland“, allerdings ist gemeinhin anerkannt, dass es sich dabei um einen Staat handelt, in dem das europäische Datenschutzrecht mangels eines entsprechenden Rechtsanwendungsbefehles nicht gilt.[1] Obwohl die Schweiz traditionell als Drittland angesehen wird,[2] formuliert das BDSG in § 1

[1] Siehe bspw. Paal/Pauly/Pauly, 2. Aufl. 2018, DSGVO Art. 44 Rn. 6.

[2] Taeger/Gabel/Schmidt, 3. Aufl. 2019, BDSG § 1 Rn. 37.

[3] Hervorhebung durch den Autor.

Abs. 6, dass „die Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum und die Schweiz den Mitgliedstaaten der Europäischen Union [gleichstehen]“.[3] Allerdings hat die Schweiz, im Gegensatz zu den Mitgliedern des Europäischen Wirtschaftsraums (EWR), die durch einen entsprechenden Beschluss aus dem Jahr 2018 den Geltungsbereich der DSGVO auf das EWR-Hoheitsgebiet erstreckt haben,[4] die Anwendbarkeit der DSGVO nicht für sich akzeptiert.

Die vom BDSG vorgesehene Gleichstellung der Schweiz mit den EU-Mitgliedstaaten und EWR-Mitgliedern ist daher europarechtswidrig.[5] Das 2. DSAnpUG-EU korrigiert dies nun und streicht die Wörter „und die Schweiz“ aus § 1 Abs. 6 BDSG. Damit gelten für Datenübermittlungen in die Schweiz zukünftig auch gemäß BDSG die Anforderungen des Kapitel V der DSGVO. In der Praxis wird sich mit dieser Änderung durch das 2. DSAnpUG-EU kein weitreichender Neujustierungsbedarf für Unternehmen ergeben, da mit dem von der Europäischen Kommission im Jahr 2000 erlassenen Angemessenheitsbeschluss[6] eine Rechtsgrundlage für Datentransfers für die Schweiz besteht.

Der Angemessenheitsbeschluss behält auch nach Geltungsbeginn der DSGVO gemäß Art. 45 Abs. 9 DSGVO seine Gültigkeit. Allerdings sollten Unternehmen prüfen, ob beispielsweise Datenschutzhinweise oder das Verzeichnis von Verarbeitungstätigkeiten im Lichte der Neueinstufung als „Drittland“ angepasst werden müssen.

2. Verarbeitung besonderer Kategorien personenbezogener Daten (§ 22 BDSG)

Durch eine Änderung des § 22 BDSG ist die Verarbeitung besonderer Kategorien personenbezogener Daten – zusätzlich zu den bereits bestehenden Rechtsgrundlagen – für Unternehmen zukünftig auch dann erlaubt, wenn diese Verarbeitung „aus Gründen eines erheblichen öffentlichen Interesses zwingend erforderlich ist“. Ausweislich der Gesetzesbegründung kann ein solches zwingendes Erfordernis zum Beispiel bei der „Verarbeitung von personenbezogenen Daten mit Religionsbezug durch zivilgesellschaftliche Träger im Rahmen von Präventions- und Deradikalisierungsprogrammen“ im Bereich des religiös motivierten Extremismus bestehen. Unternehmen, die besondere Kategorien personenbezogener Daten geschäftsmäßig im Rahmen eigener gewerblicher Geschäftsmodelle verarbeiten, können ihre Datenverarbeitung regelmäßig nicht auf diese neue Zulässigkeitsnorm stützen.[7]

3. Einwilligung im Beschäftigungsverhältnis (§ 26 BDSG)

Um die informationelle Selbstbestimmung von Beschäftigten abzusichern, hat der Gesetzgeber für das Beschäftigungsverhältnis als formelle Voraussetzung einer Einwilligung die Schriftform i.S.d. § 126 BGB angeordnet, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist (siehe § 26 Abs. 2 S. 3 BDSG). Dass dieses grundsätzliche Schriftformerfordernis von den weniger restriktiven Anforderungen der DSGVO an eine wirksam erteilte Einwilligung abweicht[8] und damit von der DSGVO eingerissene Hürden neu errichtete, ist mit guten Gründen rechtspolitisch kritisiert und vereinzelt gar als unionsrechtswidrig angeprangert worden.[9]

Mit dem 2. DSAnpUG-EU wird das in § 26 BDSG verankerte grundsätzliche Schriftformerfordernis nun abgeschafft. Die neue Fassung sieht vor, dass die Einwilligung „schriftlich oder elektronisch zu erfolgen [hat], soweit nicht wegen besonderer Umstände eine andere Form angemessen ist“.[10] Dies erleichtert die Voraussetzungen, unter denen vom Arbeitgeber im Beschäftigungsverhältnis eine Einwilligung eingeholt werden kann. Zwar sind auch nach der Neufassung mündlich oder konkludent erteilte Einwilligung nur dann zulässig, soweit dies wegen besonderer Umstände angemessen ist,[11] allerdings ist eine in dieser Form abgegebene Einwilligung mit großer Rechtsunsicherheit behaftet und damit im Beschäftigungskontext in vielen Fällen wenig attraktiv.

Summa summarum ist die Aufhebung des Schriftformerfordernisses im Beschäftigungsverhältnis zu begrüßen. Sie entspricht dem von ▶

[4] Siehe dazu Decision of the EEA Joint Committee No 154/2018 of 6 July 2019 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022]; abrufbar unter <https://www.efta.int/media/documents/legal-texts/eea/other-legal-documents/adopted-joint-committee-decisions/2018%20-%20English/154-2018.pdf>.

[5] So auch Piltz, BDSG – Praxiskommentar für die Wirtschaft, 2017, § 1, Rn. 54ff.

[6] Entscheidung der Kommission v. 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzes personenbezogener Daten in der Schweiz, 25.8.2000, ABl. L 215/1.

[7] Deutscher Bundestag, Gesetzentwurf der Bundesregierung, Drucksache 19/4674, S. 211.

[8] Siehe Art. 4 Nr. 11 DSGVO.

[9] Dazu Kühling/Buchner/Maschmann, 2. Aufl. 2018, BDSG § 26 Rn. 64; Kort, Der Beschäftigtendatenschutz gem. § 26 BDSG-neu: Ist die Ausfüllung der Öffnungsklausel des Art. 88 DSGVO geglückt?, ZD 2017, 319 (321). Überzeugender ist die Ansicht, dass das Schriftformerfordernis in § 26 BDSG von der Öffnungsklausel des Art. 88 DSGVO abgedeckt ist.

[10] Hervorhebung durch den Autor.

[11] Insofern ist auch die Neuregelung des § 26 Abs. 2 S. 3 BDSG durch das 2. DSAnpUG-EU strenger als die DSGVO.

den Koalitionsfraktionen proklamierten Ziel, alle Gesetze auf ihre „Digitaltauglichkeit" zu überprüfen.[12] Zukünftig können Einwilligungen von Arbeitnehmern problemlos per E-Mail erteilt und vom Arbeitgeber entsprechend abgespeichert werden.[13]

4. Datenschutzbeauftragte für nichtöffentliche Stellen (§ 38 BDSG)

Die wohl prominenteste und umstrittenste Änderung des BDSG durch das 2. DSAnpUG-EU betrifft die Benennungspflicht für betriebliche Datenschutzbeauftragte gemäß § 38 BDSG. Nach der aus § 4f Abs. 1 BDSG a.F. übernommenen Schwellwertgrenze müssen Verantwortliche und Auftragsverarbeiter bislang einen Datenschutzbeauftragten benennen, „soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen".

Die Unionsfraktionen hatten im Rahmen des Gesetzgebungsverfahrens die Forderung aufgestellt, diesen Schwellwert auf 50 Personen anzuheben, um insbesondere den Mittelstand von bürokratischen Belastungen zu befreien. Schlussendlich haben sich die Koalitionsfraktionen im 2. DSAnpUG-EU nun auf eine Erhöhung von zehn auf 20 Personen verständigt. Unverändert bestehen bleibt die Regelung, nach der ein Datenschutzbeauftragter unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen auch dann benannt werden muss, wenn der Verantwortliche oder Auftragsverarbeiter Verarbeitungen vornehmen, die einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO unterliegen, oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeiten.[14]

Dass mit der Heraufsetzung der Benennungsschwelle tatsächlich das vom Gesetzgeber bezweckte Ziel erreicht wird, kleine und mittlere Unternehmen sowie ehrenamtlich tätige Vereine zu entlasten,[15] darf mit guten Gründen bezweifelt werden. Denn wie bereits vielfach angemerkt, geht mit der Befreiung von der DSB-Benennungspflicht keine Entbindung von den materiellen datenschutzrechtlichen Pflichten einher. Auch das Haftungs- und Bußgeldrisiko bleibt mit den Änderungen durch das 2. DSAnpUG-EU im vollem Umfang bestehen. Die Entschärfung der Benennungspflicht trägt damit das Risiko in sich, dass „Kompetenz und Sachverstand"[16] abgebaut werden. Dies würde KMUs sowie ehrenamtlich tätigen Vereinen zumindest mittelfristig schaden.

Vor diesem Hintergrund ist auch die weitere Entwicklung kritisch zu verfolgen. Denn laut der von Bundeswirtschaftsminister Peter Altmaier (CDU) Anfang Oktober vorgelegten Mittelstandsstrategie wird sich das von ihm geführte Haus „weiter dafür einsetzen, dass die Schwelle für die Bestellung eines betrieblichen Datenschutzbeauftragten von 20 auf mindestens 50 Beschäftigte angehoben wird".[17] Auch die Europäische Kommission sieht den deutschen Sonderweg bei der DSB-Benennungspflicht kritisch. In ihrer im Juli 2019 vorgelegten Ein-Jahres-Bilanz zur DSGVO schreibt die Kommission, dass die deutsche Regelung im BDSG „zu einer Fragmentierung und zu unnötigen Belastungen führt".[18] Das letzte Wort ist in dieser Angelegenheit folglich noch nicht gesprochen.

5. Behördliches Betretensrecht (§ 40 BDSG)

Gemäß Art. 58 DSGVO verfügen die Datenschutz-Aufsichtsbehörden über eine Reihe von Untersuchungs-, Abhilfe- und Genehmigungsbefugnissen, um ihre Aufgaben ordnungsgemäß zu erfüllen. Insbesondere sind die Datenschutz-Aufsichtsbehörden gemäß Art. 58 Abs. 1 Buchst. f) DSGVO dazu ermächtigt, gemäß dem Verfahrensrecht der Union oder des Mitgliedstaats von dem Verantwortlichen oder Auftragsverarbeiter Zugang zu seinen Räumlichkeiten einschließlich aller Datenverarbeitungsanlagen und -geräte zu erhalten. Die entsprechende verfahrensrechtliche Konkretisierung im BDSG findet sich in § 40.

Mit dem 2. DSAnpUG-EU erfährt das behördliche Betretensrecht nun eine – wenn auch nur deklaratorische – Einschränkung. So wird sowohl für den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) als auch für die Aufsichtsbehörden der Länder klargestellt, dass die unternehmensseitig bestehende Pflicht zur Zugangsgewährung „nur während der üblichen Betriebs- und Geschäfts-

[12] Siehe Deutscher Bundestag, Beschlussempfehlung und Bericht des Ausschusses für Inneres und Heimat (4. Ausschuss), Drucksache 19/11181, S. 19.

[13] Ebenda.

[14] § 38 Abs. 1 S. 2 BDSG.

[15] Siehe Fn. 12, S. 19.

[16] So die GDD, Bundestag beschließt 2. DSAnpUG und ändert damit die Bestellpflicht betrieblicher Datenschutzbeauftragter gemäß § 38 BDSG, 28.6.2019; abrufbar unter <https://www.gdd.de/aktuelles/startseite/bundestag-beschliesst-2-dsanpug-und-aendert-damit-die-bestellpflicht-betrieblicher-datenschutzbeauftragter-gemaess-38-bdsg>.

[17] Bundesministerium für Wirtschaft und Energie, Wertschätzung – Stärkung – Entlastung, Mittelstandsstrategie, 1.10.2019, S. 10; abrufbar unter <https://www.champions-von-hier.de/CHAMPS/Redaktion/DE/Publikationen/mittelstandsstrategie.pdf?__blob=publicationFile&v=6>; Hervorhebung durch den Autor.

[18] Europäische Kommission, Datenschutzvorschriften als Voraussetzung für Vertrauen in die EU und darüber hinaus – eine Bilanz, 24.7.2019, COM(2019) 374 final, S. 4.

[19] Ausweislich der Gesetzesbegründung wirkt die Änderung des § 16 Abs. 4 BDSG über den Verweis in § 40 Abs. 5 Satz 3 BDSG auch klarstellend für die Aufsichtsbehörden der Länder; siehe Fn. 7, S. 210.

zeiten“ gilt.[19] Laut Gesetzesbegründung wird damit den verfassungsgerichtlichen Anforderungen an das behördliche Betretensrecht Rechnung getragen.[20] In der Praxis wird die Änderung allerdings keine Auswirkungen zeitigen, da sich die zeitliche Begrenzung auf die Betriebs- und Geschäftszeiten bereits aus dem europarechtlich normierten Grundsatz der Verhältnismäßigkeit ergibt.[21]

III. Ausgebliebene Änderungen des BDSG

1. Videoüberwachung durch Private (§ 4 BDSG)

Das Bundesverwaltungsgericht (BVerwG) hat in einem Urteil aus dem März 2019 festgestellt, dass die in der DSGVO enthaltenen Öffnungsklauseln Videoüberwachungen privater Verantwortlicher nicht erfassen.[22] Folglich fehlte dem deutschen Gesetzgeber die Gesetzgebungskompetenz für den Erlass des § 4 BDSG (Videoüberwachung öffentlich zugänglicher Räume) zur Regelung solcher privater Videoüberwachungsmaßnahmen. Weshalb die Entscheidung des BVerwG im Gesetzgebungsverfahren zum 2. DSAnpUG-EU trotz entsprechender Forderungen aus der Opposition offenbar gänzlich unberücksichtigt blieb, ist unklar.

2. Beschäftigungsdatenschutz und Recht auf freie Meinungsäußerung (Art. 88, 85 DSGVO)

Auch an anderen Stellen wurde eine Chance zur Nachbesserung des BDSG vertan. So besteht erheblicher Regelungsbedarf hinsichtlich der Datenverarbeitung im Beschäftigungskontext (Art. 88 DSGVO) sowie hinsichtlich des Ausgleichs zwischen dem Recht auf freie Meinungsäußerung und des Schutzes personenbezogener Daten (Art. 85 DSGVO).[23] Im Hinblick auf Art. 85 DSGVO hat der Innenausschuss des Deutschen Bundestages die Bundesregierung nun aufgefordert, zügig einen Regelungsvorschlag vorzulegen. In diesem Zusammenhang wurde die Bundesregierung ebenfalls gebeten, zu prüfen, „ob und in welchem Umfang bisher zentrale Regelungen wie zum Beispiel das Kunsturhebergesetz (KunstUrhG) und das Telemediengesetz (TMG) auch nach dem 25. Mai 2018 fortgelten“.[24]

3. Meldung von Datenschutzverletzungen (§ 43 BDSG)

Im Bereich der Meldung von Datenschutzverletzungen belässt es der Gesetzgeber bei der aktuellen Vorschrift in § 43 BDSG. Danach darf eine Meldung oder Benachrichtigung aufgrund einer Datenschutzverletzung nach Art. 33, 34 DSGVO in einem Bußgeldverfahren gegen das betreffende Unternehmen „nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden“. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg geht davon aus, dass § 43 BDSG europarechtswidrig ist[25] und wendet diesen in seiner Bußgeldpraxis offenbar nicht an.

4. Aufsichtsbehördliche Befugnisse im Bereich der Berufsgeheimnisträger (§ 29 BDSG)

Auch der weitgehende Ausschluss der Untersuchungsbefugnisse der Datenschutz-Aufsichtsbehörden bei zahlreichen Berufsgeheimnisträgern (insbesondere Ärzten, Rechtsanwälten) gemäß § 29 Abs. 3 BDSG ist vom Gesetzgeber trotz massiver Kritik[26] nicht neu geregelt worden. Dass sich diese Regelung noch in den Grenzen der unionsrechtlichen Öffnungsklausel des Art. 90 DSGVO bewegt, darf bezweifelt werden.[27]

Über den Autor

Dr. iur. Tilman M. Dralle, LL.M. (Nottingham)

Senior Consultant mit den Schwerpunkten IT-Compliance, Datenschutz und Informationssicherheit bei TÜV Rheinland

▶ https://www.tuv.com/germany/de/

TÜVRheinland®
Genau. Richtig.

[20] Ebenda.

[21] Siehe Erwägungsgrund 129 DSGVO. Vgl. auch Paal/Pauly/Körffer, 2. Aufl. 2018, DSGVO Art. 58 Rn. 14; BeckOK DatenschutzR/Eichler, 29. Ed. 1.5.2019, DSGVO Art. 58 Rn. 15.

[22] BVerwG 6 C 2.18, Urteil v. 27.3.2019, Ziff. 47.

[23] Siehe insbesondere die Stellungnahme der EAID v. 16.7.2018 zum 2. DSAnpUG-EU; abrufbar unter <https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/stellungnahmen/zweites-dsanpug-eu-omnibus/stellungnahme-eaid_dsanpug-eu-2.pdf?__blob=publicationFile&v=3>.

[24] Fn. 12, S. 16.

[25] Siehe z.B. LfDI BW, 33. Tätigkeitsbericht 2016/2017, S. 17.

[26] So z.B. Fn. 23, S. 1-2.

[27] So auch Kühling/Buchner/Dix, 2. Aufl. 2018, BDSG § 40 Rn. 15.

DER ERLAUBNISTATBESTAND DES § 26 BDSG

Heiko Schöning, LL.M.

Einleitung

Mit dem „Beschäftigtendatenschutz nach neuem Recht" befasst sich Stefan Sander in seinem Beitrag in der Privacy in Germany (PinG) 2019, Seite 127 ff. Nachfolgend fasst der Autor die wesentlichen Ergebnisse von Sander zusammen und stellt diese auch in den Kontext der selbst unter den Aufsichtsbehörden derzeit umstritten Frage, ob im Rahmen der – isoliert betrachteten – Lohn- und Gehaltsbuchhaltung durch Steuerberater eine Auftragsverarbeitung gemäß Art. 28 DSGVO stattfindet.

Nicht behandelt wird die umstrittene Frage, ob eine Auftragsverarbeitung entweder "automatisch" entsteht, wenn die zu betrachtende Tätigkeit den gesetzlich beschriebenen Anforderungen genügt, also der Auftraggeber sinngemäß über die Mittel und Zwecke der Verarbeitung bestimmt und die „organisatorischen Pflichten nachgelagert zu vereinbaren sind" gemäß der Anforderungen des Art. 28 DSGVO. Oder ob die Auftragsverarbeitung und die (insoweit auch umstritten) immanente Privilegierung (früher: § 3 Abs. S. 2 Nr. 3 i.V.m. § 3 Abs. 8 S. 3 BDSG aF) der an der Auftragsverarbeitung Beteiligten nur durch den Abschluss eines Vertrages (oder anderen Rechtsinstruments) gemäß der Vorgaben des Art. 28 Abs. 3 DSGVO unter Einhaltung der in Art. 28 Abs. 9 DSGVO genannten Formalia entsteht.

Ausgangspunkt der hier zu behandelnden Fragestellung ist, wer sich als „Verantwortlicher" auf die Ermächtigungsgrundlage des § 26 BDSG berufen kann. Gilt die Norm nur für Verarbeitungen, die unmittelbar im Verhältnis zwischen dem (möglicherweise zukünftigen, aktuellen oder ehemaligen) Arbeitgeber und dem Arbeitnehmer erfolgen? Oder anders ausgedrückt: Kann sich jemand als eigener Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO auf § 26 BDSG für die Verarbeitung von personenbezogener Daten – ggfs. auch und insbesondere besonderer personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO – berufen, ohne dass der Betroffene jemals in einem unmittelbaren arbeitsrechtlichen Vertragsverhältnis mit diesem „Dritten" stand, steht oder eventuell zukünftig stehen wird?

Es gibt Stimmen in der Literatur, die im Wesentlichen die Ansicht vertreten, dass § 26 BDSG auch in Bezug auf Verarbeitungen durch Verantwortliche greifen würde, die in keinem „Beschäftigungsverhältnis" i.S.v. § 26 BDSG zum Betroffen stehen (siehe Nachweise bei Sander, a.a.O.).

§ 26 Abs. 8 S. 1 BDSG zählt zum einen (abschließend) auf, wer als „Beschäftigter" im Sinne der Norm anzusehen ist. Dies sind in Folge der expliziten Benennung auch Leiharbeitnehmer im Verhältnis zum Entleiher; obwohl diese gerade nicht Arbeitnehmer des Entleihers sind; der Verleiher überträgt lediglich für die Dauer der vereinbarten Arbeitnehmerüberlassung das Weisungsrecht an den Entleiher (vgl. § 1 Abs. 1 S. 2 AÜG), bleibt aber weiterhin Arbeitgeber. Zum anderen wird in § 26 Abs. 8 S. 2 BDSG klargestellt, dass Bewerber

für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist, als Beschäftigte gelten.

Als Ausgangspunkt der Diskussion zur oben gestellten Frage ist wohl die nachfolgend zitierte Textstelle aus dem Aufsatz von Wybitul in der Neue Zeitschrift für Arbeitsrecht (NZA) 2017, Seite 413, [414] zu nennen:

> *„Seinem Wortlaut nach richtet sich § 26 [BDSG] als Normadressaten nicht alleine an Arbeitgeber, sondern allgemeiner an sämtliche Verantwortliche, die personenbezogene Beschäftigtendaten im Beschäftigungskontext verarbeiten. (...) Damit gilt § 26 [BDSG] nicht nur für Stellen, die betroffene Personen iSv § 26 VIII [BDSG] beschäftigen, sondern gegebenenfalls auch für Auftragnehmer oder Dritte, die für den Arbeitgeber personenbezogene Daten im Beschäftigungskontext verarbeiten."*

Folgt man der zitierten Auslegung der Norm durch Wybitul, der sich zustimmend weitere Stimmen in der Literatur angeschlossen haben (Sander, a.a.O, Fn. 10 mwN), können insbesondere auch Dritte i.S.v. Art. 4 Nr. 10 DSGVO in eigener Verantwortlichkeit personenbezogene Daten eines Beschäftigungskontextes verarbeiten, sofern die weiteren Voraussetzungen des § 26 BDSG eingehalten sind, obwohl sie nicht Arbeitgeber (oder Entleiher) des betroffenen Beschäftigten sind. Die Frage ist also, wie weit geht die Bedeutung der Worte „*Beschäftigungskontext*" (Art. 88 DSGVO) bzw. „*für Zwecke des Beschäftigungsverhältnisses*" (§ 26 BDSG)?

Die Auslegung der Norm

Anders als Art. 6 Abs. 1 lit. f DSGVO, der im Rahmen der möglichen Interessenabwägung explizit einen Dritten und dessen Interessen benennt, fehlt in § 26 Abs. 1 BDSG ein solcher Verweis. Lediglich die „Interessenvertretung der Beschäftigten" wird genannt, wobei es umstritten ist, ob der Betriebsrat (bzw. Personalrat) Teil des Verantwortlichen oder eigener Verantwortlicher ist (offen gelassen vom BAG, Beschl. v. 09.04.2019 – Az. 1 ABR 51/17, Rn. 47 mwN).

Sofern man den Betriebsrat als eigenen Verantwortlichen ansieht, wäre er zwar Dritter, aber auch ausdrücklich in § 26 Abs. 1 DSGVO genannt. § 26 Abs. 3 BDSG statuiert, dass abweichend von Art. 9 Abs. 1 DSGVO die Verarbeitung besonderer Kategorien personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses zulässig ist, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.

Somit muss die Verarbeitung für Zwecke des Beschäftigungsverhältnisses erforderlich sein und es dürfen keine schutzwürdigen Interessen der betroffenen Person entgegenstehen. Aufgrund des Verweises in § 26 Abs. 3 S. 3 BDSG ist die Regelung des § 22 Abs. 2 BDSG, wonach angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen sind, bei der Abwägung der Interessen entsprechend zu beachten (BAG, a.a.O., Rn. 40).

Der jeweilige Wortlaut der verschiedenen Absätze des § 26 BDSG ergibt kein eindeutiges Auslegungsergebnis.

Indes zeigt die systematische Betrachtung, dass ein spezifischer Dritter, nämlich der Entleiher, vom Gesetzgeber als Arbeitgeber angesehen wird (§ 26 Abs. 8 S. 1 Nr. 1 BDSG).

Ferner hat der Gesetzgeber Dritte, sofern diese von einer Ermächtigungsgrundlage erfasst sein sollen, explizit benannt (wie z.B. in Art. 6 Abs. 1 lit. f DSGVO).

Damit können sich unter systematischen Gesichtspunkten Dritte nicht auf den Erlaubnistatbestand des § 26 BDSG für Verarbeitungen in eigener Verantwortlichkeit berufen.

Die Verarbeitung von besonderen Kategorien personenbezogener Daten, wie z.B. Gesundheitsdaten oder Angaben zur religiösen Überzeugung, bedarf einer gesonderten Erlaubnis nach Art. 9 Abs. 2 DSGVO bzw. diese muss sich auf die Öffnungsklausel des Art. 9 Abs. 4 DSGVO stützen können. Letztere würde aber infolge des eindeutigen Wortlauts die Verarbeitung von personenbezogenen Daten zur religiösen Überzeugung nicht mehr abdecken, sodass für den Abzug der „Kirchensteuer" diese Angabe nicht mehr im Bereich der Lohnsteuerberechnung und -abfuhr ▸

verarbeitet werden dürfte; nach Art. 9 Abs. 2 lit. b DSGVO i.V.m. § 26 Abs. 3 BDSG ist dies grundsätzlich zulässig, weil der Arbeitgeber gesetzlich verpflichtet ist, die Lohnsteuer für die Arbeitnehmer abzuführen.

Sander kommt zu dem Ergebnis, wonach „die Auslegung des § 26 BDSG (…) eindeutig [ergibt], dass sich nur derjenige Verantwortliche zur Rechtfertigung einer durch ihn (bzw. i. S. v. Art. 28 DSGVO für ihn) ausgeführten Verarbeitung stützen kann, der in einem Beschäftigungsverhältnis zur betroffenen Person steht."

Ein wesentlicher Punkt seiner Argumentation ist, dass es ansonsten zu Rechtsunsicherheiten kommt, welche Verarbeitung eines eigenverantwortlichen Dritten sich noch im „Beschäftigungskontext" bewegt und welche nicht mehr. Beispielhaft werden neben der bereits angesprochenen Lohn- und Gehaltsbuchhaltung auch einige weitere denkbare Anwendungsfälle skizziert, wo zwar abstrakt noch ein irgendwie geartetes Näheverhältnis zum „Beschäftigungskontext" gesehen werden könnte, die „Verkehrsauffassung" diese Ansicht aber wohl nicht mehr teilen wird. Wäre der Beschäftigungskontext noch zu bejahen,

- wenn der Logistikdienstleister Archivräume bereitstellt für die Einlagerung von Personalakten zum Zwecke von deren Aufbewahrung?
- wenn ein Rechenzentrumsdienstleister, der IT-Ressourcen für HR-Systeme oder eine Lösung für elektronische Lohnabrechnungen, digitales Bewerbermanagement oder on- bzw. off-boarding Prozesse bereitstellt?
- wenn ein Möbelhändler infolge einer Anfrage oder Bestellung des Arbeitgebers Kenntnis von einer Rückenerkrankung eines Beschäftigten erfährt, weil letzterer z.B. in den Geschäftsräumen des Händlers verschiedene Modelle von höhenverstellbaren Tischen und besonders rückenschonende Stühlen im Rahmen eines vereinbarten Termins persönlich ausprobiert?

Fazit

Gerade auch im Hinblick auf die nicht abschließend beispielhaft aufgezeigten Fälle kann die Frage, ob sich ein Verantwortlicher auf § 26 BDSG stützen kann, durch das leicht überprüfbare Kriterium, ob zwischen dem Verantwortlichen und der betroffenen Person ein Beschäftigungsverhältnis vorliegt, eindeutig beantwortet werden. Auch wenn es aus Sicht der Praxis zunächst unbefriedigend erscheint, so ist zu konstatieren, dass der Gesetzgeber zum einen noch andere Erlaubnisnormen bereithält und zum anderen die DSGVO (hoffentlich) im Nachgang der Evaluation (vgl. Art. 97 DSGVO) punktuelle „Verbesserungen" erhält.

Die schwierige Einwilligung wird – neben denjenigen Verarbeitungen, die als Auftragsverarbeitung gemäß Art. 28 DSGVO realisiert werden können – zukünftig vermehrt zum Einsatz kommen. Auch wenn der EuGH mit seinen letzten Entscheidungen vom 29.07.2019 – C-40/17-„FashionID" (zur Frage „wer" eine Einwilligung einholen muss) und 01.10.2019 – C-673/17-„Planet49" (zur Frage was muss bei der Einholung einer Einwilligung beachtet werden) die zu beachtenden Anforderungen nicht gerade „Verarbeiter-freundlich" geurteilt hat.

Über den Autor

Heiko Schöning

LL.M. betrieblicher Datenschutzbeauftragter, Rechtsanwalt und Fachanwalt für IT-Recht und Partner bei SDS Rechtsanwälte Sander Schöning PartG mbB in Duisburg.

▶ www.sds.ruhr

sds Rechtsanwälte Sander Schöning PartG mbB

SCORING – VORAUSSETZUNGEN UND BETROFFENENRECHTE NACH DER DSGVO UND DEM BDSG

Daniel Joos

Für die Bewertung des Zahlungsverhaltens, insbesondere beim Abschluss von Kreditverträgen, werden oftmals Auskünfte über die Bonität des potentiellen Vertragspartners bei Auskunfteien eingeholt. Dabei greifen die Auskunfteien regelmäßig auf sogenannte Scorings zurück, im Kern also statistisch-mathematische Verfahren unter Verwendung eines Wahrscheinlichkeitswertes, um das künftige (Zahlungs-) Verhalten einer Person zu prognostizieren. Der vorliegende Beitrag soll einen Überblick über die dogmatische Einordnung des „Scorings", die rechtlichen Rahmenbedingungen sowie mögliche Betroffenenrechte unter Datenschutzgesichtspunkten darstellen.

I. Einleitung

Gem. § 31 Abs. 1 S. 1 BDSG wird Scoring definiert als „[d]ie Verwendung eines Wahrscheinlichkeitswerts über ein bestimmtes zukünftiges Verhalten einer natürlichen Person zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dieser Person (…)".[1] Schon aus der gesetzlichen Überschrift des § 31 BDSG, „Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften", ergibt sich die Intention des nationalen Gesetzgebers, dem „Wirtschaftsverkehr" Methoden an die Hand zu geben, um das zukünftige Verhalten eines potentiellen Vertragspartners abschätzen zu können. Auch aus der Gesetzesbegründung zu § 31 BDSG ergibt sich ausdrücklich, dass durch die Novellierung erreicht werden sollte, „welche Voraussetzungen ein von einer Auskunftei ermittelter Score-Wert im Hinblick auf sog. Negativ-Merkmale erfüllen muss, damit er im Wirtschaftsverkehr verwendet werden darf".[2]

Daraus ergibt sich ein klares Leitbild des nationalen Gesetzgebers, wonach die Nutzung von Scorewerten über die Bonität beziehungsweise Kenntnisse über (abschlägiges) Zahlverhalten des Vertragspartners für den Wirtschaftsverkehr unerlässlich sind. ▸

[1] Vgl. § 31 Abs. 1 S. 1 BDSG
[2] BT-Drs. 18/11325, S. 101

Die Gesetzesbegründung spricht im Rahmen der Ermittlung der Bonität sogar vom „Fundament des deutschen Kreditwesens“ und dem Schutz der „Verbraucher vor Überschuldung“.[3]

Dies mag mit Blick auf kurzfristig, schnell und ohne vertragliche Vorbeziehung zu fällende Entscheidungen im Bereich der Kreditvergabe, des Versandhandels oder der Wohnraummiete ein nachvollziehbares Interesse sein, wird von Datenschützern allerdings nicht als unkritisch angesehen. Zum einen hat der Betroffene von vornherein kaum Handhabe hinsichtlich der durch die Auskunfteien gespeicherten Daten, also auch nicht ob diese falsch oder unvollständig sind oder ob Daten, welche zugunsten des Betroffenen sprechen könnten, fehlen. Zudem können auch sogenannte Schätzungen oder Vergleichsparameter Einzug in den Scorewert finden.

II. Rechtlicher Rahmen nach der DSGVO

Auch die DSGVO enthält Normen zur Problematik des Scoring, jedoch unter der Terminologie des „Profiling“. Gem. Art. 4 Nr. 4 DSGVO ist Profiling *„jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen“*.[4]

Ein Profiling liegt somit vor, wenn die Persönlichkeitsaspekte die Grundlage der automatisierten Verarbeitung bilden, mit dem Ziel, neue Informationen und Kenntnisse über die Persönlichkeit zu erhalten oder zu bewerten.[5]

Beim Scoring handelt es sich somit um eine spezielle Form des Profilings.[6]

Gem. Art. 22 Abs. 1 DSGVO hat der Betroffene zudem das Recht, nicht *„ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden“*.[7] Gem. Art. 22 Abs. 2 lit. b DSGVO gilt dies allerdings gerade nicht in Fällen, wo die Entscheidung *„für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist“*[8] oder eine Ausnahme im nationalen Recht vorgesehen ist.

Nach Art. 22 Abs. 2 lit. b DSGVO können die Mitgliedsstaaten somit Ausnahmen und abweichende Vorschriften über die Anwendung von Profiling erlassen.[9] Von dieser Öffnungsklausel hat Deutschland durch die Novellierung des § 37 BDSG für die Versicherungswirtschaft[10] und in § 31 BDSG Gebrauch gemacht.

III. Scoring nach dem BDSG

§ 31 Abs. 1, Abs. 2 BDSG regelt, unter welchen Mindestvoraussetzungen ein Scorewert zu errechnen ist, damit der Empfänger ihn zur Grundlage einer Entscheidung machen darf. Zuvorderst sind hierbei die *„Vorschriften des Datenschutzes“* einzuhalten.[11] Im Grundsatz kann sich eine Auskunftei dabei auf Art. 6 Abs. 1 lit. f DSGVO berufen und alle personenbezogenen Daten erheben, speichern und nutzen, die für die Berechnung des Scores geeignet und erforderlich sind, wobei auf die berechtigten Interessen Dritter Rücksicht zu nehmen ist.[12]

[3] BT-Drs. 18/11325, S. 101

[4] Vgl. Art. 4 Nr. 4 DSGVO

[5] Scholz in Simitis, Datenschutzrecht, 1. Aufl. 2019, Art. 4 Nr. 4, Rn. 6

[6] Scholz in Simitis, Datenschutzrecht, 1. Aufl. 2019, Art. 22, Rn. 24

[7] Vgl. Art. 22 Abs. 1 DSGVO

[8] Vgl. Art. 22 Abs. 2 lit. b DSGVO

[9] Buchner in Kühling / Buchner, DSGVO, 1. Aufl. 2017, Art. 22, Rn. 37

[10] Vgl. Wortlaut von § 37 Abs. 1 BDSG („Leistungserbringung nach einem Versicherungsvertrag“)

[11] Vgl. § 31 Abs. 1 Nr. 1 BDSG

[12] Ehmann in Simitis, Datenschutzrecht, 1. Aufl. 2019, Anhang 2 zu Art. 6, Rn. 17

1. Grundvoraussetzung: Richtigkeit der Datenbestände

Als elementarste Grundvoraussetzung des Scorings ist selbstverständlich die „Richtigkeit" der Daten zu nennen (vgl. auch Art. 18 Abs. 1 lit. a DSGVO). Die Problematik des von der Auskunftei zu Grunde zu legenden Datensatzes stellt sich in der Realität jedoch oftmals als sehr schwer überprüfbar dar. Zunächst ist es nicht auszuschließen, dass es zu Namensverwechslungen kommt. Hinsichtlich der verwendeten Daten haben sich einige Grundsätze herausgebildet. Demnach dürfen nicht „*begründungslos*" unzutreffende oder nur oberflächliche Fakten berücksichtigt werden.[13] Ferner dürfen keine höchstpersönlichen Angaben (Daten nach Art. 9 DSGVO) wie Gewerkschaftszugehörigkeit oder religiösen Einstellung berücksichtigt werden. Ein weiterer Streitpunkt ist die Hinzuziehung „öffentlicher Daten". Diese wird man sicherlich nicht per se der Verwendung beim Scoring entziehen können, da sie im Einzelfall auch Anhaltspunkte zu Gunsten des Betroffenen enthalten können. Insbesondere beim Bonitätsscoring kann durch Einsicht in Schuldnerverzeichnis der Vollstreckungsgerichte (vgl. § 882f Abs. 1 Satz 1 Nr. 4, § 882g Abs. 2 Nr. 2 ZPO) oder ähnliche „öffentliche" Register eine gewisse Sicherheit bewerkstelligen lassen.[14] Schwierig ist jedoch die Frage zu beantworten, ob darüber hinaus auch auf andere „öffentlich zugängliche" Quellen zurückgegriffen werden darf. Das Interesse der Auskunfteien an Social-Media-Daten ist vor dem Hintergrund der umfassenden (Selbst-) Darstellung der Betroffenen in sozialen Medien nachvollziehbar, aber mit Blick auf das Recht auf Privatsphäre kritisch.[15] Außerdem fließen oftmals auch „*soziodemographische Merkmale*" in die Bewertung ein.[16] Dabei handelt es sich um Merkmale wie Anschrift, Familienstand, Bildungsgrad oder die Anzahl der Kinder, was auch als kritisch bewertet wird.[17]

2. Voraussetzungen des § 31 Abs. 1 Nr. 1 bis Nr. 4 BDSG

In § 31 Abs. 1 Nr. 1 bis Nr. 4 BDSG sind vier Negativ-Merkmale normiert, welche kumulativ vorliegen müssen.[18] Dabei handelt es sich unter anderem um Anforderungen an die Wissenschaftlichkeit der Formel beziehungsweise das Verbot der ausschließlichen Nutzung von Anschriftendaten.[19]

3. Scoring über Zahlungswilligkeit / -fähigkeit

Konkret für das Bonitätsscoring, also die Bewertung der Zahlungswilligkeit oder -fähigkeit einer natürlichen Person, enthält das BDSG in § 31 Abs. 2 BDSG weitere Voraussetzungen. Ausdrücklich normiert werden in den Nr. 1 bis Nr. 5 die Anforderungen, welche an die konkret einzubeziehenden Forderungen zu stellen sind, wie etwa die Fälligkeit der Forderung, Anerkenntnis oder denkbare Vollstreckungstitel.[20] Diese Verpflichtung trifft auch die Unternehmen, welche Forderungen in den Datenbestand der Auskunfteien „einmelden".[21]

IV. Betroffenenrechte

Die DSGVO hält in den Art. 15 ff. Betroffenenrechte bereit, die gegenüber den Verantwortlichen geltend gemacht werden können.

1. Recht auf Auskunft gem. Art. 15 DSGVO

Dem Betroffenen steht zuvorderst das Recht auf Auskunft über die ihn betreffenden verarbeiteten personenbezogenen Daten nach Art. 15 DSGVO zu. Art. 15 DSGVO ist als zentrales Betroffenenrecht die Grundlage für die Geltendmachung der weiteren Betroffenenrechte.[22]

2. Recht auf Berichtigung gem. Art. 16 DSGVO

Nach Art. 16 DSGVO hat der Betroffene zudem das Recht auf Berichtigung. Das bedeutete, dass im Falle des Widerspruchs die Auskunftei den Datensatz auf seine Richtigkeit hin überprüfen und gegebenenfalls berichtigen muss.[23] Ist es der Auskunftei nicht möglich die Richtigkeit zu beweisen, müssen die Angaben entweder berichtigt oder gelöscht werden.[24]

3. Einsicht in die Scoreformel

Bei den gängigen Scoringverfahren handelt es sich um statistisch-mathematische Verfahren, welche anhand von Wahrscheinlichkeitswerten und Vergleichsparametern Prognosen generieren. Betroffene haben daher neben der Auskunft über die verwendeten Daten oder die Nutzer der Scorewerte auch oftmals das Interesse, mehr über das verwendete Scoringverfahren zu ▶

[13] OLG Frankfurt, Urt. v. 07.04.2015 – 24 U 82/14

[14] Krämer NJW 2018; 347, 349

[15] 25. Tätigkeitsbericht Datenschutz 2014/2015 des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI), S. 222

[16] Handreichung „Verbraucher-Scoring" des Unabhängige Landeszentrums für Datenschutz Schleswig-Holstein (ULD), S. 6, Stand: Mai 2010

[17] Handreichung „Verbraucher-Scoring" des ULD, S. 6,

[18] Piltz in Piltz / BDSG, 1. Aufl. 2018, § 31 BDSG, Rn. 7

[19] Vgl. § 31 Abs. 1 Nr. 2, Nr. 3 BDSG

[20] Ehmann in Simitis, Datenschutzrecht, 1. Aufl. 2019, Anhang 2 zu Art. 6, Rn. 76

[21] 25. Tätigkeitsbericht Datenschutz 2014/2015 des HmbBfDI, S. 216

[22] Bäcker in Kühling / Buchner DSGVO, 1. Aufl. 2017, Art. 15 Rn. 5

[23] Vgl. zur alten Rechtslage: Meents/ Hinzpeter in Taeger/ Gabel BDSG, § 35 BDSG aF., Rn. 8 ff.

[24] Vgl. Art. 16 DSGVO; Art. 17 Abs. 1 lit. d DSGVO

erfahren. Der 63. Erwägungsgrund zur DSGVO billigt dem Betroffenen grundsätzlich zu, zu erfahren *„nach welcher Logik die automatische Verarbeitung personenbezogener Daten erfolgt und welche Folgen eine solche Verarbeitung haben kann (...)"*.[25] Gleichzeitig handelt es sich bei den verwendeten Scoreverfahren um aufwendig und teuer entwickelte Anwendungen, welche zum Geschäftsgeheimnis der Auskunftei zählen. Auch der Bundesgerichtshof entschied noch unter alter Rechtslage zum Auskunftsanspruch gegen die Auskunftei SCHUFA nach § 34 Abs. 4 Satz 1 Nr. 4 BDSG aF., dass der Auskunftsanspruch sich nicht auf die Scoreformel an sich und damit die *„eingeflossenen allgemeinen Rechengrößen"* bezieht.[26] Der BGH stellte in seinem Urteil wohl darauf ab, dass die Scoreformel zum Geschäftsgeheimnis der SCHUFA gehöre und ansonsten im Wege der Auskunft an den Betroffenen, „durch die Hintertür" an Wettbewerber geraten könnte. In jedem Fall trage die Socreformel zur Wettbewerbsfähigkeit bei und definiere den *„Marktwert des Produkts und der Auskunftei selbst"*.[27]

Dieser Gedanke ist im Grundsatz auch der DSGVO immanent, da durch das Recht auf Auskunft nach Art. 15 DSGVO *„Geschäftsgeheimnisse oder Rechte des geistigen Eigentums und insbesondere das Urheberrecht an Software, nicht beeinträchtig[t]"* werden sollen.[28] Einen Anspruch auf konkreten Einblick in die Scoreformel besteht somit nicht.

V. Zusammenfassung

Neben den beschriebenen Fällen im Bereich der Kreditvergabe hat Scoring auch Anwendungsfälle in vielen anderen Bereichen, wie beispielsweise des Versandhandels, der Werbebranche, der Wohnraumvermittlung aber auch bei KFZ-Leasingverträgen.[29] Vor dem Hintergrund der beschriebenen Problemfelder ist verantwortlichen Nutzern von Scorings und Kundenunternehmen von Auskunfteien zu raten, bei der Meldung und Übermittlung von Daten die vorgenannten Datenschutzgesichtspunkte einzuhalten und ihre Mitarbeiter dahingehend zu schulen. Betroffenen ist zu raten, von ihrem Recht auf Auskunft Gebrauch zu machen, um die für sie gegebenenfalls nachteiligen Folgen abschätzen und im Bedarfsfall weitere Schritte einleiten zu können. Viele Aufsichtsbehörden oder Verbraucherorganisationen halten hierzu Musterschreiben zur Orientierung vor.[30]

Über den Autor

Daniel Joos

arbeitet im Referat IV „Datenschutz im nicht-öffentlichen Bereich" beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg

▶ www.baden-wuerttemberg.datenschutz.de

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

[25] Erwägungsgrund 63 zur DSGVO, S. 3

[26] BGH, Urt. v. 28.01.2014 – VI ZR 156/13

[27] BGH, Urt. v. 28.01.2014 – VI ZR 156/13

[28] Erwägungsgrund 63 zur DSGVO, S. 5

[29] Piltz in Piltz / BDSG, 1. Aufl. 2018, § 31 BDSG, Rn. 1

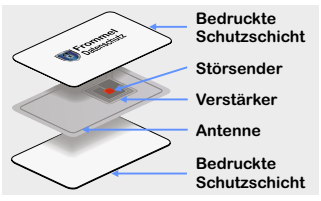
[30] So auch der LfDI BW auf dem Internetauftritt: www.baden-wuerttemberg.datenschutz.de

Anzeige

Ihr Name kann Kundendaten schützen!

Frommel Multimedia

Kennen Sie das Problem mit dem drahtlosen Datenklau?
Weitere Informationen unter: www.frommel.com/nfc
Abhilfe leisten sogenannte NFC/RFID-Blockerkarten.



Vorteile von NFC/RFID-Blockerkarten:

- **Schützt vor unbefugtem Datenabgriff per NFC/RFID**
- **Zum Schutz eine Karte pro Portemonnaie mitführen**
- **Ververwendbar als Visitenkarte (Abmessungen: 85 x 55 mm)**
- **Freie grafische Gestaltung und beidseitiger Farbdruck**
- **Ihr Kunde trägt die Kontaktdaten des DSB immer mit sich**
- **Nützliches, beliebtes und geniales Werbegeschenk**

Frommel Multimedia • Telefon: 06172-1710179 • 06172-1714896 • E-Mail: info@frommel.com • www.frommel.com

WEBSEITEN NACH DER DSGVO: LÄNGERE DATENSCHUTZERKLÄRUNGEN UND MEHR COOKIE-HINWEISE.

Martin Degeling und Christine Utz

Die Medienaufmerksamkeit rund um die Einführung der Datenschutzgrundverordnung hat dazu geführt, dass viele Unternehmen sich (erstmals) Gedanken darüber gemacht haben, ob und wie sie Datenschutzvorgaben auf ihren Webseiten umsetzen. In zwei Studien haben wir – Wissenschafter*innen der Ruhr-Universität Bochum und der University of Michigan – untersucht, wie sich Internetseiten durch die DSGVO verändert haben und wie die weit verbreiteten Cookie-Hinweise von Nutzer*innen wahrgenommen werden.

Dazu wurden von Dezember 2017 bis zum Sommer 2018 die 500 meistbesuchten Webseiten aller europäischen Mitgliedsstaaten monatlich automatisiert aufgerufen und die Verwendung von Cookies und HTTPS sowie etwaigen Datenschutzerklärungen abgerufen. Im Anschluss haben wir verschiedene Varianten von Cookie-Hinweisen auf einer realen Website mit rund 80.000 Besucher*innen evaluiert.

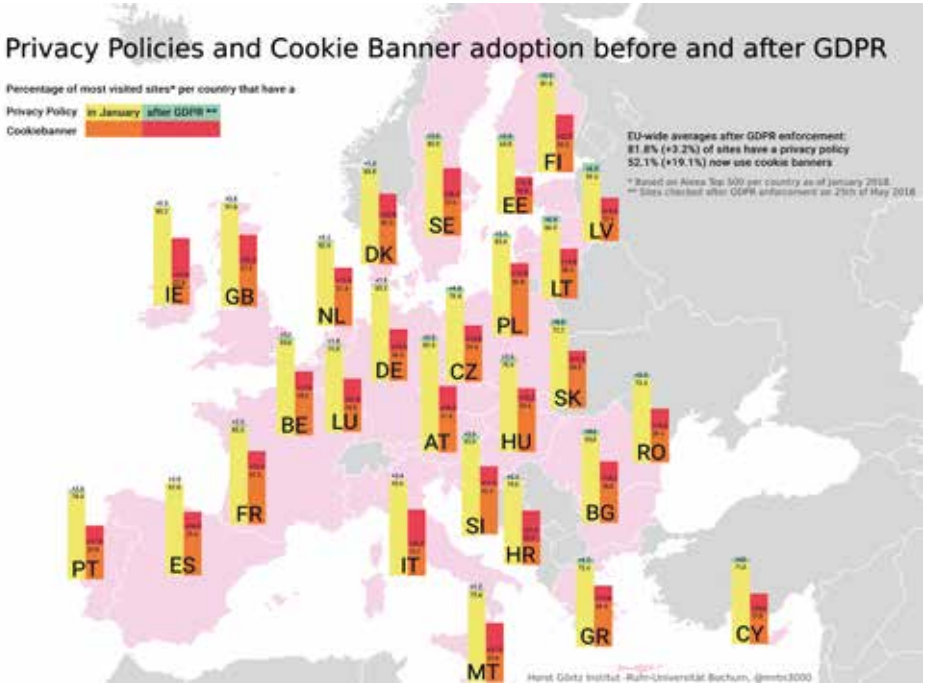
Mehr Webseiten haben eine Datenschutzerklärung.

Ein positives Ergebnis der ersten Untersuchung ist, dass schon vor der Datenschutzgrundverordnung die meisten Webseiten eine Datenschutzerklärung vorweisen konnten. Im Januar 2018 fanden wir auf fast 80 Prozent der Webseiten eine, wenn auch nicht unbedingt ausführliche, Datenschutzerklärung. Der Wert schwankte zwischen 60 Prozent in Litauen und 95 Prozent in Großbritannien. In Deutschland lag er bei 89 Prozent.

Mit der endgültigen Einführung der DSGVO stieg der Durchschnittswert um fünf Prozent, wobei insbesondere Webseiten, die in den baltischen Staaten häufig besucht werden, nun (endlich) um Datenschutzerklärungen ergänzt wurden.

In Deutschland konnten wir einen Anstieg um drei Prozent beobachten. ▸

Während die zunehmende Transparenz bezüglich der Datenverarbeitung auf Webseiten einerseits positiv zu bewerten ist, zeigen unsere Messungen auch, dass die Entwicklung nicht unbedingt im Sinne der Betroffenen ist. Die Länge von Datenschutzerklärungen stieg im gleichen Zeitraum von 2.145 auf 3.044 Wörter. Das heißt, dass die Erklärungen im Durchschnitt über 40 Prozent länger geworden sind. Häufig wurden sie dabei kaum inhaltlich überarbeitet, sondern nur um Abschnitte mit Bezug zur DSGVO ergänzt. Weitere Beobachtungen ergaben, dass sich die Anzahl der verwendeten Drittanbieter-Skripte und Cookies kaum verändert hat, so dass nicht weniger Daten weitergegeben werden. Positiv entwickelt hat sich hingegen die standardmäßige Nutzung von HTTPS, die im Untersuchungszeitraum von 60 auf 80 Prozent anstieg.



Die auffälligste Änderung war allerdings der sprunghafte Anstieg bei der Verbreitung von Cookie-Hinweisen. Von den 6.357 untersuchten Webseiten hatten im Januar 2018 zunächst 46 Prozent und im Mai schon 62 Prozent einen Cookie-Hinweis. In Ländern wie Italien oder Irland betrug der Anstieg gar über 40 Prozent. In Deutschland stieg die Rate von 26 auf 49 Prozent – ein Effekt der Lesart des TMG, die bis zum „Planet49"-Urteil des Europäischen Gerichtshofs vor wenigen Wochen die Nutzung von Cookies auch ohne Einwilligung ermöglichte. Aber das Einbinden eines Cookie-Hinweises bedeutet noch nicht, dass eine Webseite auch eine (gültige) Einwilligung nach der DSGVO einholt. Unsere Detailanalyse vom August 2018 zeigt, dass nur 14 Prozent der Webseiten in ihrem Cookie-Hinweis überhaupt die Möglichkeit boten, nicht einzuwilligen. Der Großteil der Webseiten weist die Nutzer*innen auch heute noch nur auf die Verwendung von Cookies hin, ohne eine Möglichkeit zur Abwahl zu bieten. Bedenklich ist ferner, dass 57 Prozent der Hinweise die Seiten-Besucher*innen zur Einwilligung drängen, indem die Option zur Zustimmung grafisch hervorgehoben ist oder, wie im „Planet49"-Fall, Checkboxen vorausgewählt sind.

Bei genauerer Betrachtung zeigt sich, dass dies auch ein technisches Problem ist. Über 40 Prozent der von uns untersuchten Programmbibliotheken zur Einbindung eines Cookie-Hinweises bieten gar keine Option, einen aktiven Opt-In durchzusetzen. Selbst wenn den Nutzer*innen also Auswahloptionen angeboten wurden, lud die Seite Dienste von Drittanbietern direkt beim Aufruf und setzte Cookies.

Cookie Hinweise: Ungeliebt und unpraktisch

In einer zweiten Studie haben wir untersucht, wie Webseitenbesucher*innen Cookie-Hinweise nutzen Dazu haben wir eine eigene Implementierung eines Cookie-Hinweises für die Content-Management-Plattform WordPress so angepasst, dass sie verschiedene, weit verbreitete Varianten von Cookie-Hinweisen anzeigen kann, von einfachen informierenden Dialogboxen bis zum An- und Abwählen aller in die Website eingebundenen Drittanbieter.

Getestet wurde, wie die Nutzer*innen mit den Hinweisen abhängig von deren Position auf dem Bildschirn, den angebotenen Auswahlmöglichkeiten und dem Text interagierten. Bei der Position wurden neben den weit verbreiteten „Banner"-Varianten am oberen oder unteren Rand des Browserfensters auch solche Gestaltungen getestet, bei denen der Hinweis in einer Dialogbox in einer der Ecken des Bildschirms erscheint. Auf mobilen Geräten wurden die Hinweise jeweils am oberen und unteren Rand getestet.

In einem ersten Experiment mit knapp 14.000 Nutzer*innen auf einer deutschen E-Com-

merce-Webseite konnten wir beobachten, dass die meisten versuchten, den Hinweis zu ignorieren – selbst auf mobilen Geräten, wo der Hinweis einen beträchtlichen Teil des Bildschirms einnimmt. Nur 37 Prozent gaben oder verweigerten die Einwilligung. In einer anschließenden Umfrage zeigten sich viele der Befragten frustriert von Cookie-Hinweisen und ein Viertel der Teilnehmer*innen berichteten, dass sie Cookies aus Sorge akzeptieren, dass die Webseite sonst nicht funktionieren würde. Tatsächlich führen einzelne schwarze Schafe, die Cookie-Ablehnenden den Zugang zur Webseite versperren, dazu, dass viele Cookies blind akzeptieren oder versuchen, die Hinweise zu ignorieren.

In einem zweiten Versuch mit über 30.000 Teilnehmer*innen wurden die Auswahlmöglichkeiten variiert. Dabei unterschieden wir zwischen Hinweisen ohne jegliche Auswahlmöglichkeit, solchen, die ausschließlich eine Bestätigung anbieten (z. B. „ok" oder „verstanden"), Hinweisen mit zwei Auswahlmöglichkeiten („akzeptieren" und „ablehnen") und zwei Varianten, bei denen die Nutzer*innen explizit bestimmte Drittanbieter an- bzw. abwählen konnten. Diese wurden entweder nach Zweck gruppiert (z. B. „Soziale Medien" oder „Marketing") oder es wurden alle Anbieter einzeln mit Namen aufgelistet. Alle Varianten wurden dann jeweils in einer zur Zustimmung drängenden und in einer neutralen Version getestet. Zur Zustimmung drängend heißt, dass Checkboxen vorausgewählt sind und Buttons, die zur Zustimmung führen, hervorgehoben dargestellt werden.

Tatsächlich zeigt sich hier der größte Einfluss auf das Klickverhalten der Webseiten-Besucher*innen.. Insbesondere bei komplexeren Hinweisen mit Checkboxen steigt die Zustimmung deutlich, wenn diese vorausgewählt sind. Während nur eine niedrige einstellige Zahl an Nutzer*innen jegliche Form von Cookies aktiv auswählt, werden sie von über 30 Prozent akzeptiert, wenn sie vorausgewählt sind. Den geringsten Effekt hatten die Beeinflussungsversuche, wenn Nutzer*innen nur zwei Auswahlmöglichkeiten („akzeptieren" und „ablehnen") zur Verfügung standen.

In einem letzten Test mit weiteren 32.000 Nutzer*innen wurde untersucht, inwiefern der Text der Cookie-Hinweise einen Einfluss auf die Entscheidungen hat. Dazu wurden Varianten getestet, die einen oder keinen Link zur Datenschutzerklärung enthielten, sowie solche in technischer („Diese Seite verwendet Cookies") oder nicht-technischer Sprache („Diese Seite erhebt von Ihnen Daten …"). Die Ergebnisse zeigen, dass das Klickverhalten bezogen auf die Antwortmöglichkeiten vom Text unbeeinflusst ist, allerdings war die Interaktionsrate mit dem Cookie-Hinweis am höchsten, wenn das Wort „Cookie" im Text erwähnt wurde.

Im Ergebnis bleibt festzustellen, dass die Nutzung von Cookie-Hinweisen seit der Einführung der Datenschutzgrundverordnung rapide zugenommen hat. Zusammen mit immer längeren Datenschutzerklärungen führt dies aktuell eher zu einer Überforderung der Nutzer*innen, die teilweise große Einschränkungen bei der Verwendung der Seiten in Kauf nehmen, um keine Entscheidung für oder gegen Cookies treffen zu müssen. Datenschutzfreundliche Webseiten, die standardmäßig ohne Cookies auskommen oder Opt-in-Verfahren implementieren, könnten die Interaktion hier deutlich vereinfachen. Hier sind aber auch die Entwickler*innen von „DGSVO-Plugins" und ähnlichen Diensten gefragt, die häufig diese Anforderungen nicht erfüllen. Langfristig sinnvoll erscheint eine browserbasierte Lösung ähnlich zu Do-Not-Track, über die zumindest ein Großteil der Abfragen vorab beantwortet werden könnte.

Über die Autoren

Martin Degeling
ist Post-Doktorand und Mitarbeiter am Horst Görtz Institut für IT-Sicherheit der Ruhr-Universität Bochum. Seine Forschung beschäftigt sich mit den Auswirkungen der Datenschutzgrundverordnung auf Webseiten sowie Transparenz von und Schutz vor Online-Tracking und Profiling.

Christine Utz
ist Doktorandin am Horst Görtz Institut für IT-Sicherheit der Ruhr-Universität Bochum. Ihre Forschung beschäftigt sich mit der technischen Umsetzung vom Datenschutzgesetzen, Datenökonomie und Usable Privacy.

▶ www.hgi.rub.de

hgi
Horst Görtz Institut
für IT-Sicherheit

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. (2019). We Value Your Privacy … Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy. Proc. NDSS 2019.

Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)informed Consent: Studying GDPR Consent Notices in the Field. Proc. CCS '19.

SCHUTZ VON HOCHSENSIBLEN DATEN: SCHREDDERN IST NICHT GLEICH SCHREDDERN

Wendela Freiesleben

Digitalisierung wird weltweit vorangetrieben. Trotzdem produzieren Unternehmen in Deutschland noch Tonnen von Papier. Laut einer Viadesk Studie drucken allein Führungskräfte durchschnittlich 40 DIN-A4-Seiten pro Tag. Diese Papierflut muss auch entsorgt werden. Akten und Dokumente mit personenbezogenen Daten dürfen seit der neuen EU-Datenschutzgrundverordnung (DSGVO) nicht einfach im Papierkorb landen, sie müssen – idealerweise mit einem modernen Schredder - entsorgt werden. Unternehmen, die sich nicht an diese Regeln halten, drohen erhebliche Bußgelder wegen einer Ordnungswidrigkeit nach Artikel 83 DSGVO.

Eine aktuelle Studie von LEITZ ACCO Brands zeigt, dass 71 Prozent der Unternehmen ihren Datenschutz noch nicht auf die physische Vernichtung von Papierunterlagen angepasst haben. 53 Prozent haben bestätigt, im Zuge der neuen Gesetzgebung noch keine Geräte zum Schreddern von Papier gekauft zu haben. Dabei gelten besonders in den Bereichen der Medizin, Justiz oder auch Forschung höchste Anforderungen in Sachen Datenschutz. Die DIN-Norm 66399 kategorisiert die Vernichtung von Papierdokumenten in drei Schutzklassen. Zusätzlich gibt es sieben Sicherheitsstufen. Sie regeln wie klein die Akten zerschnitten werden müssen. Beides muss im Hinblick auf die zu schützenden Daten gewählt werden. Für geheim zu haltende Daten wie medizinische Berichte oder auch Mandanteninformationen wird die Sicherheitsstufe P5 vorgeschrieben, für Forschungs- oder Entwicklungsunterlagen sogar P6. Datenschutzbeauftragten in Unternehmen oder Behörden müssen je nach zu vernichtenden Unterlagen auf Modelle mit den Sicherheitsstufen P4 bis P6 zurückgreifen.

Studie bestätigt: Geringe Kenntnis über Sicherheitsstufen

In Unternehmen besteht laut Datenschutzexperten wie Wolf-Rüdiger Heidemann vom TÜV Süd noch eine große Unsicherheit in Sachen Datenschutz und Aktenvernichtung. Dies bestätigt auch die Studie von LEITZ ACCO Brands, bei der 40 Prozent der 600 befragten Entscheidungsträger für den Einkauf von Bürogeräten glauben, dass sich die DSGVO nur auf digitale Daten auswirkt. 41 Prozent der Befragten kennen die Sicherheitsstufen für die Aktenvernichtung überhaupt nicht.

Daher hat die Premium-Büromarke LEITZ, die zu den weltweit führenden Anbietern von Büroprodukten gehört, acht neue hochwertige Aktenvernichter der LEITZ IQ-Serie entwickelt, die in Sachen Sicherheit deutlich über den gesetzlichen Vorschriften liegen. Sie starten mindestens ab der Sicherheitsstufe DIN-P4. Die Geräte P5, P5+ und P6+ sind auf hohe Sicherheitsanforderungen ausgerichtet und bieten auch bei sensiblen Daten Schutz. Je nach Modell können fünf bis sieben DIN-A4-Seiten auf einmal zerkleinert werden. So werden Akten schnell und fast geräuschlos geschreddert. Normale Heft- und Büroklammern müssen dabei nicht entfernt werden. Das Spitzenmodell P6+ schreddert eine A4 Seite sogar in über 12.000 kleine Partikel. Das sind doppelt so viele, wie die DIN-Norm P6 fordert. Damit können die Daten absolut sicher vor dem Zugriff Unbefugter entsorgt werden.

Ein weiteres Problem bei der Aktenvernichtung ist, dass laut LEITZ ACCO Brands-Studie fast jedes zweite Unternehmen immer noch keinen oder nur einen einzigen Aktenvernichter hat. Damit nehmen Unternehmen in Kauf, gegen Geheimhaltungsvorschriften zu verstoßen und bringen zudem die Betroffenen, deren Daten nicht mehr geschützt sind, in Gefahr, Opfer von Betrug und Identitätsdiebstahl zu werden. Wenn Unterlagen einfach im Papierkorb landen, bietet das keinen Schutz mehr. Stattdessen sollten sich Unternehmen Gedanken darüber machen, jeden Mitarbeiter, der regelmäßig mit sensiblen Daten umgeht, einen leistungsfähigen Aktenvernichter unter den Schreibtisch zu stellen. Damit wird der Schredder zum modernen „Papierkorb 2.0".

Über die Autorin

Wendela Freiesleben
ist Regional Marketing Director bei LEITZ ACCO Brands.

▶ www.leitz.com

BvD e.V.
DATENSCHUTZ GESTALTEN

30 Jahre BvD

Gemeinsam für einen starken Datenschutz!

30 Jahre Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. fördert seit 30 Jahren die beruflichen Interessen der Datenschutzbeauftragten in Behörden und Betrieben und setzt sich aktiv für die weitere Akzeptanz des Berufsbildes „Datenschutzbeauftragter“ ein – als einziger Verband in Deutschland.

Der BvD in Zahlen:

- gegründet 1989
- Mitglieder: 1.870
- Firmenmitglieder: 1.145
- bundesweit 11 Regionalgruppen und 9 Arbeitskreise zu Fachthemen

(Stand: Oktober 2019)

BERUFSVERBAND DER DATENSCHUTZBEAUFTRAGTEN DEUTSCHLANDS (BVD) E. V. | BUDAPESTER STRASSE 31, 10787 BERLIN
TELEFON: (030) 26 36 77 60 | TELEFAX: (030) 26 36 77 63 | E-MAIL: BVD-GS@BVDNET.DE | INTERNET: WWW.BVDNET.DE

DATEV-STIFTUNG ZUKUNFT IST WIEDER BEI DER DAME DABEI

Interview mit Dr. Sebastian Sprenger

Katrin Eggert

Zum zweiten Mal fördert die DATEV-Stiftung Zukunft den Datenschutz Medienpreis (DAME) des BvD, der im Frühjahr 2020 zum dritten Mal vergeben wird. Über das besondere Engagement für den Preis und die Ziele der DATEV-Stiftung Zukunft in Sachen Datenschutz sprachen die BvD-News mit Stiftungs-Mitarbeiter Dr. Sebastian Sprenger.

BVD-News: *Im vergangenen Jahr hat die DATEV-Stiftung Zukunft ihre Unterstützung für den BvD ausgebaut. Sie sind seitdem Mitglied in der Jury unserer DAME. Welchen Eindruck haben Sie bisher gewonnen?*

Sebastian Sprenger: Der Datenschutz Medienpreis ist eine sehr spannende Angelegenheit. Die Möglichkeit, Teil der Jury sein zu dürfen, freut mich sehr. Anfangs wusste ich zugegebenermaßen nicht wirklich, was mich erwartet. Ich konnte mir bis dato schlichtweg nur sehr schwer vorstellen, wie man das Thema Datenschutz mit Hilfe audiovisueller Medien und in einem kreativen Prozess darstellen könnte. Als ich dann aber die Fülle und Tiefe der Beiträge zu sehen bekam, die von den Bewerbern eingereicht wurden, dachte ich nur, diese Idee, einen Datenschutz Medienpreis auszuloben, ist genau der richtige Weg, um nachhaltig Aufmerksamkeit für das Thema Datenschutz zu erzeugen. Ich kann deshalb nur dazu aufrufen, sich die Arbeiten der Sieger, aber auch der anderen Bewerber anzusehen und sich mit den Inhalten zu beschäftigen. Wenn diese Filme es im Ergebnis schaffen, das eigene Verhalten zu reflektieren, dann ist das Ziel eines solchen Preises absolut erreicht.

BVD-News: *Der BvD zählt zu den ersten Förderpartnern der DATEV-Stiftung Zukunft. Was macht diese Partnerschaft aus Ihrer Sicht so wertvoll, dass sie nun bereits seit über vier Jahren besteht?*

Sebastian Sprenger: Wir arbeiten mit dem BvD ganz bewusst schon mehrere Jahre zusammen. Wir sind im Rahmen der Initiative „Datenschutz geht zur Schule" gestartet und ich durfte bereits selbst einige der ehrenamtlich aktiven Dozenten kennenlernen, die vor Kindern und Jugendlichen für einen bewussten und selbstbestimmten Umgang mit persönlichen Daten in der digitalen Welt eintreten. Wir befürworten dieses Engagement ausdrücklich. Das zeigt sich nicht zuletzt auch darin, dass das Kuratorium der DATEV-Stiftung Zukunft über die Fortführung einer Zusammenarbeit jedes Jahr neu entscheiden muss. Man sieht also, dass die Gremien der DATEV-Stiftung sehr überzeugt sind von den gemeinnützigen Projekten des BvD.

BVD-News: *Ende 2014 gründete die DATEV die gemeinnützige DATEV-Stiftung Zukunft. Wie kam es überhaupt dazu?*

Sebastian Sprenger: Der Vorstand der DATEV hat damals überlegt, wie man den Genossenschaftsmitgliedern zum 50-jährigen Jubiläum der DATEV etwas zurückgeben kann. Am besten natürlich etwas, was länger wirkt als einmalige Geschenke. So kam die Idee auf, eine Stiftung zu gründen und mit dieser Stiftung Ziele zu verfolgen, die langfristig und damit natürlich auch nachhaltig unseren genossenschaftlichen Mitgliedern zu Gute kommen. Nach reiflichen Überlegungen und vielen Gesprächen wurde schließlich im Dezember 2014 die Gründungsurkunde gemeinsam mit unserem Geschäftspartner, der Deutschen Stiftungstreuhand, unterzeichnet.

BVD-News: *Welche Ziele verfolgt die Stiftung?*

Sebastian Sprenger: Wenn wir in diesen Tagen über „Digitalisierung" reden, dann schwenkt der Fokus allzu oft auf Themen zu innovativen Produkten und disruptiven Geschäftsmodellen, sprich: wie kann man in einer digitalen Wirtschaftswelt in Zukunft als Unternehmen überleben und mit welchen Produkten und Dienstleistungen lässt sich künftig Geld verdienen? Die DATEV-Stiftung Zukunft stellt den Mensch in den Mittelpunkt in solch bewegten Zeiten. Wir wollen unter anderem dazu beitragen Anforderungen einer künftigen Berufswelt besser zu verstehen. Wie werden sich bestimmte Berufsbilder entwickeln und welche Kompetenzen werden zunehmend in Unternehmen gebraucht? Und natürlich nehmen Themen aus den Bereichen IT-Sicherheit und Daten-

schutz eine sehr wichtige Position ein. Was bedeutet „digitale Souveränität" und wie kann selbstbestimmtes Handeln in einer vernetzten Welt gewährleistet werden? Darüber hinaus ist uns auch das Thema „Vernetzung und Zusammenarbeit" ein sehr großes Anliegen.

BVD-News: *Das klingt auf jeden Fall ambitioniert. Wie erreicht die DATEV-Stiftung Zukunft diese Ziele?*

Sebastian Sprenger: In erster Linie unterstützen wir Vereine, Organisationen und Institutionen bei der Umsetzung ihrer Ideen. Wir fördern derzeit zehn Projekte parallel, alle beschäftigen sich auf unterschiedliche Weise mit einem Teilaspekt der bereits genannten Ziele der DATEV-Stiftung. Mit dem Dr.-Heinz-Sebiger-Preis für herausragende Promotionsarbeiten verleihen wir außerdem einen eigenen Förderpreis. Der Großteil unserer Arbeit besteht aber darin, Förderpartner finanziell bei der Umsetzung ihres Vorhabens zu unterstützen.

Wir sind davon überzeugt, dass die Verwirklichung unserer Stiftungszwecke dann am besten gelingt, wenn wir die Umsetzung in den Händen derjenigen Personen belassen, die sich inhaltlich am besten auskennen. Natürlich besprechen wir im Vorfeld die gemeinsame Erwartungshaltung für das jeweilige Projekt, aber unsere Förderpartner sollen weitestgehend frei in der Realisierung ihrer Ideen sein. Das ist für uns sehr wichtig und bewahrt die Authentizität.

BVD-News: *Was bedeutet Datenschutz für Sie persönlich?*

Sebastian Sprenger: Ich denke, ich erzähle nichts Neues, wenn ich behaupte, dass Leben und Arbeiten bereits heute in sehr gewichtigem Maße online stattfinden. Je stärker diese Durchdringung sein wird, desto sicherer muss sich jeder Einzelne von uns souverän und selbstbestimmt in einer solchen Welt fortbewegen können. Wenn wir beispielsweise unsere Wohnung online ummelden, dann wollen wir sicher sein, dass die angegebenen Daten auch nur in den Händen Berechtigter landen. Das gilt auch, wenn wir uns online auf eine Jobanzeige bewerben. Und vermutlich haben auch die wenigsten Nutzer von Dating Plattformen ein Interesse daran, dass ihre Angaben über das Portal hinaus an Dritte weitergegeben werden. Dass der Nutzer solchen Vorgängen aber oftmals unwissend zustimmt, ist Ergebnis fehlender Sensibilität und – was oft viel schwerer wiegt – wenig praktikabler Umsetzungen durch die Betreiber. Wir müssen in einer digitalisierten Welt die Zusammenhänge verstehen und Konsequenzen unseres Handelns bewusst ableiten können. Und dabei sehe ich es als verpflichtend an, dass Politik und Wirtschaft miteinander daran arbeiten, die richtigen Voraussetzungen hierfür zu schaffen.

Dr. Sebastian Sprenger
ist Referent der DATEV-Stiftung Zukunft und verantwortet das operative Geschäft der Stiftung.
▶ www.datev.de

Über die Autorin

Katrin Eggert
verantwortet für den BvD die Projekte „Datenschutz geht zur Schule" sowie den Datenschutz Medienpreis.

Die DAME des BvD

Der Datenschutz Medienpreis des BvD geht in die dritte Runde. Fast 30 Produzenten, Redakteurinnen, Jugendliche und YouTuber haben sich mit ihren Produktionen um die mit 3.000 Euro dotierte Auszeichnung beworben.

Die Jury aus Datenschutz- und Medienexperten nominiert im Februar 2020 drei Bewerber oder Teams. Sie reisen zur Preisgala am 6. Mai nach Berlin, auf der die Jury die finalen Gewinner bekannt gibt. Die feierliche Preisübergabe findet im Rahmen der BvD-Verbandstage in Berlin statt.

VON GUTER LAUNE UND LECKERBISSEN

Herbsttagung und Behördentag 2019 in Nürnberg

Christina Denz

Die Nachfrage nach der BvD-Herbstkonferenz wächst. 300 Teilnehmende hatten sich in diesem Jahr für „Wirtschaft trifft Aufsicht“ am 23. und 24. Oktober angemeldet, so viele wie noch nie. Damit alle die Vorträge auf der Hauptbühne verfolgen konnten, musste ein Ausweichraum mit Live-Übertragung dazugebucht werden.

„Auf der Konferenz kann man sehr gut Tendenzen der Rechtsauslegung bei den Aufsichtsbehörden einfangen. Vor allem die Aufsichtsbehörden in Bayern geben einige zielführende Fragen und Antworten, das ist auch für mich aus Schleswig-Holstein interessant. Hier erhalte ich Denkanstöße, die mir helfen, an unsere zuständige Aufsichtsbehörde die richtigen Fragen zu stellen.“

Gitta Lau
W&P Plus

Erstmals hatte die Herbstkonferenz und der Behördentag am 25. Oktober im Le Meridien Grand Hotel von Nürnberg Quartier bezogen, einem 1885 gebauten Komplex, der mit Kronleuchtern, Marmorwänden und goldfunkelnden Nischen an eine vergangene Reise-Kultur erinnerte.

Die Gastgeber – BvD-Vorstandsvorsitzender Thomas Spaeing, der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Dr. Stefan Brink, und der Präsident des Bayerischen Landesamts für Datenschutzaufsicht, Thomas Kranig, – eröffneten die Tagung, die in diesem Jahr unter dem Motto „Konsens oder Konflikt – wo geht's lang“ stand.

Heribert Prantl, Kolumnist, Jurist und wortgewandte Verfechter von Rechtsstaat und Bürgerrechten warnte in seiner Key-Note vor einer gefährlichen Totalität durch Überwachung und Datenspeicherung.

„Der Kontakt mit den Aufsichtsbehörden ist außerordentlich wichtig. Wenn es diese Gelegenheit nicht gäbe, wäre ich nicht nach Nürnberg gekommen. Die Chance, Fragen zu stellen und direkt Antworten von den Aufsichtsbehören zu bekommen, hilft sehr.“

Bernd Herrig
Technische Akademie für berufliche Bildung Schwäbisch-Gmünd

„Ich erlebe die Aufsichtsbehören auf der Konferenz als sehr auskunftsfreudig. Ich selbst stelle gerne kritische Fragen, bin aber damit in Nürnberg nie abgewiesen worden. Das es bei strittigen Themen dann mitunter keine konkreten Antworten gibt, liegt in der Natur der Sache.“

Alexander Politz
Braun & Paul IT GmbH

Unter Berufung auf die Innere Sicherheit würden umfangreiche Daten von Fluggästen und Bürgern gesammelt. Aber wenn nach jedem Terroranschlag Gesetze verschärft und mehr Daten gespeichert würden, werde der „Terrorist zum Gesetzgeber“. Datenschutz sei kein „Gnadenrecht“, sondern ein Grundrecht, die digitale Revolution dürfe nicht zur digitalen Inquisition werden, mahnte er.

„Die Konferenz bietet eine gute Möglichkeit zu sehen, wie die Aufsichtsbehörden arbeiten. Man bekommt auch informell viele Infos mit, die einem helfen, die eigenen Fälle besser zu beurteilen.“

Dr. Eljalill Tauschinsky
dacuro GmbH (Walldorf)

Über Datenethik und die Verantwortung von Unternehmen, auch beim Datenschutz Position zu beziehen, sprach die Medienprofessorin Dr. Petra Grimm von der Hochschule für Medien in Stuttgart. ▸

BvD-Herbstkonferenz 2019 in Nürnberg
Fotos: BvD e.V / Uli Schneider

Die Konzerndatenschutzbeauftragte der Deutschen Bahn, Chris Newiger, die zugleich Beauftragte für den Datenschutz bei den Konzernunternehmen der Bahn ist, berichtete aus ihrem Berufsalltag, auch davon, dass die Datenschutzbeauftragten Bürokratie in Unternehmen verringern, statt sie zu erhöhen.

Damit traf sie ein Kernthema, dass nach der Rede von Bayerns Innenstaatsministers Joachim Herrmann (CSU) zum Behördentag am Freitag für offene Diskussionen sorgte. Denn er kündigte an, er wolle sich im Zuge der DSGVO-Evaluierung im nächsten Jahr für einen weiteren „Bürokratieabbau" bei der DSGVO für die Wirtschaft einsetzen.

„Die Zusammenarbeit mit den Aufsichtsbehörden ist für mich immer förderlich. Dass man auf der Konferenz auf dem kurzen Dienstweg und im persönlichen Gespräch auch kontroverse Fragen erörtern und sofort nachhaken kann, dafür komme ich zur Herbsttagung. Und für meine Aufsichtsbehörde in Schleswig-Holstein kann ich hier die besseren Argumente sammeln, wenn ich weiß, wie andere Aufsichtsbehörden spezielle Fragen sehen."

Karin de Lange
behördliche Datenschutzbeauftragte
Kreis Stormarn

Im Mittelpunkt beider Tagungen stand aber der direkte Austausch mit den Aufsichtsbehörden und ihren Mitarbeitern. Neben Brink und Kranig stellte sich auch die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, Helga Block, den Fragen der Konferenz-Besucher.

„Auf der Konferenz sind viele Mitarbeiter von Aufsichtsbehörden vertreten. Wenn man weiß, wen man ansprechen muss, hat man hier die Gelegenheit dazu."

Britta Seidl
Datenschutz individuell

„Der Austausch mit den Aufsichtsbehörden hier auf der Konferenz schafft Vertrauen für einen späteren Kontakt mit der eigenen zuständigen Aufsichtsbehörde."

Thomas Goost
Syndikusanwalt bei BNP Parisbas S.A.
Niederlassung Deutschland

Mit den Aufsichtsbehörden gab es ein fleißiges Netzwerken während und nach den Vorträgen, auf dem Abendempfang im festlichen Saal und in den Fluren bei Kaffee und Snacks. „Ich spreche gerne mit den Aufsichtsbehörden, weil wir immer etwas über Themen erfahren, die uns selbst bei der Beratung weiterhelfen", sagte Christian Seehafer, Geschäftsführer der Comp4U GmbH, den BvD-News. „Ich habe auch gezielt Vertreter der Aufsichtsbehörden zu konkreten Fällen angesprochen. Die Kontakte hier zu pflegen ist sehr gut – und auch einfach."

Die Reden und Präsentationen der BvD-Herbstkonferenz „Wirtschaft trifft Aufsicht" 2019 sowie des Behördentags finden Sie auf der Website des BvD unter Verband/BvD-Herbstkonferenz Datenschutz.

Über den QR-Code gelangen Sie direkt zu den Vorträgen und Präsentationen

Über die Autorin

Christina Denz
ist Journalistin, Kommunikationsberaterin und Redakteurin der „BvD-News".

DIE DIGITALE TRANSFORMATION BRAUCHT NEUE SECURITY-STANDARDS.

INDUSTRIE 4.0 UND IoT NEUE MÖGLICHKEITEN BERGEN NEUE GEFAHREN.

IT taucht immer dort auf, wo das Geschäft stattfindet. Das heißt, alle User, Applikationen und Daten sind ständig in Bewegung. Agilität und Flexibilität gewinnen gegenüber der Stabilität immer mehr an Bedeutung. IT Security wird nicht mehr durch einen konkreten Ort definiert. Deshalb muss Security überall dort sein, wo immer IT stattfindet.

Das gilt heute besonders für das IoT in der Industrie und Wirtschaft. Ob Supermärkte, Geldautomaten oder ganze Airlines – wer die Effizienz der Technologie nutzen will, muss wissen, wie er sie schützen kann. Denn dort, wo ein derartiges Effizienzpotenzial liegt, finden sich unzählige Gefahrenpotenziale für die Sicherheit. Hierbei können existenzbedrohende Risikofaktoren entstehen. Das „Internet of Things“ ist auf die „Security of Things“ angewiesen.

Genau hierfür bietet DREGER IT Lösungen an, die höchste Sicherheit und echte Mehrwerte für Ihr Unternehmen gewährleisten.

Darüber hinaus profitieren Sie von Mehrwerten und Services, die individuell auf die Bedürfnisse Ihres Unternehmens zugeschnitten sind.

D-BUSINESS®
MONITORING

IHR MEHRWERT DURCH PROAKTIVE FEHLERERKENNUNG.

Ziel des D-BUSINESS® Monitoring ist es, Ihre IT-Abteilung zu unterstützen und für höchste Sicherheit zu sorgen. Es soll einen reibungslosen Betrieb Ihrer Infrastrukturen, Betriebssysteme und Anwendungen gewährleisten.

D-BUSINESS®
MANAGED SECURITY

IHR MEHRWERT DURCH EIN SOLIDES SICHERHEITSFUNDAMENT.

Mit dem richtigen Konzept können Sie die Sicherheit Ihrer Infrastruktur auf ein solides Fundament stellen. Unzureichend geschützte Informationen sind ein häufig unterschätzter Risikofaktor, der existenzbedrohend werden kann. Dabei sind ein vernünftiger Informationsschutz und die Grundsicherung der IT schon mit verhältnismäßig geringen Mitteln zu erreichen.

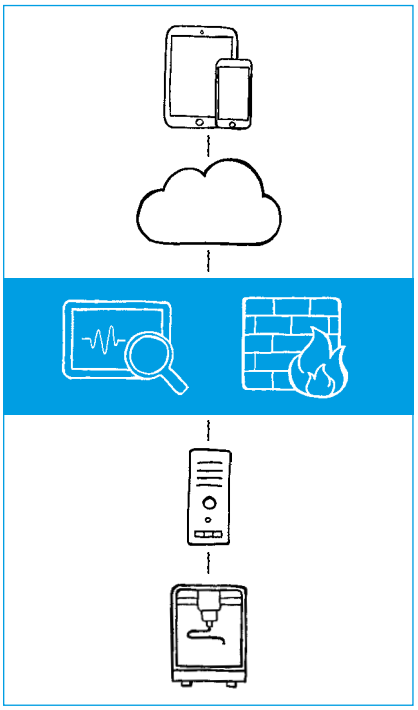
D-BUSINESS®
MANAGED IoT

UNSERE LÖSUNGEN FÜR IHRE IoT-INFRASTRUKTUR.

Mit den Produkten D-BUSINESS® Monitoring und D-BUSINESS® Managed Security erreichen Sie für Ihre IoT-Infrastruktur maximale Sicherheitsstandards bei einer gleichzeitig hohen Entlastung für die IT-Abteilung Ihres Unternehmens.

DREGER IT gewährleistet:

- Sichere Konnektivität und Überwachung der Geräte
- Erhöhung der Sicherheit durch Mikrosegmentierung, Isolierung von potenziell unsicheren Gräten
- Bedienung durch Nicht-IT-Personal (Fachabteilungen) möglich, daher keine zusätzliche Belatung der IT-Abteilung
- Reduzierung bzw. Beschleunigung des Wartungsaufwands für den Betrieb von IoT-/Industrielösungen



DREGER IT bietet Ihnen mit über 25 Jahren Erfahrung in der IT Branche, zuverlässige Services bei höchstem Datenschutz. Das beinhaltet mandantenfähige Cloud Services ohne lange Vertragsbindungen mit individuell angelegten Infrastrukturen. Zudem stehen Plattformen oder Anwendungen mit der Option auf Überwachung und Support modular zur Verfügung.

Das DREGER IT Rechenzentrum stellt Ihnen eine Vielfalt standardisierter modularer Komponenten bereit, die je nach Anforderung individuell zusammengestellt und anpassbar sind. Sie entscheiden hierbei, wie viel Verantwortung Sie an DREGER IT abgeben möchten.

DREGER Consulting GmbH & Co. KG
Hanauer Landstraße 182a
60314 Frankfurt am Main
Telefon: 069-90479-0
info@dreger.de

www.dreger.de
www.folderflex.de

DREGERIT
MACHT ES EINFACH.

JUBILÄUM AUF DEM DOZENTENTREFFEN VON DSGZS

Rudi Kramer

Seit zehn Jahren sind die ehrenamtlichen Dozentinnen und Dozenten von „Datenschutz geht zur Schule“ (DSgzS) nun bundesweit unterwegs. Seit sechs Jahren können der BvD und der AK Schule die Dozenten im Herbst zu einem Dozententag einladen, seit vier Jahren dank der großzügigen Unterstützung der DATEV Stiftung Zukunft. Ziel ist der gemeinsame Austausch und die Möglichkeit, sich bei der Sensibilisierung von Schülerinnen und Schülern gegenseitig zuhören zu können.

Am Vortag des diesjährigen Treffens in Paderborn gab es einen „Aktionstag“: Elf Dozenten gingen in das Theodoranium Gymnasium und konnten in 14 Veranstaltungen rund 300 Schülerinnen und Schüler der Jahrgangsstufe 7 erreichen. Wer danach noch wollte, hatte die Möglichkeit, an einer sehr interessanten Stadtführung durch Paderborn teilzunehmen. Der Abend klang aus mit einem gemeinsamen Besuch eines Bierlokals bei regionaler Küche.

Für den Dozententag selbst waren wieder verschiedene Vorträge vorgesehen mit medienpädagogischen und datenschutzrechtlichen Bezügen. Auch wenn es kurzfristige gesundheitsbedingte Absagen einzelner Referenten gab, konnte doch ein vielfältiges Programm geboten werden.

Zu Beginn wurde ein Grußwort der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, Helga Block, verlesen. Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, Dr. Stefan Brink, sandte eine Videobotschaft, in der er weitere Aspekte hinsichtlich des Schutzes von Kindern und deren Interessenswahrung ausführte, so auch zu der Frage, wer Kinder vor den teils exzessiven Veröffentlichungen von Bildern und Informationen über sie im Internet durch die eigenen Eltern schützt.

Danach stellte Miriam Ruhenstroth von mobilsicher e.V. ein automatisches Prüfverfahren des Datensendeverhaltens von Android-Apps vor, das angeregt diskutiert wurde. Gerd Fauser von der Hugo Boss AG bereicherte im Anschluss mit der Weitergabe der Analyse seiner Untersuchung des Einsatzes eines Messangers-Dienstes im Unternehmensumfeld die Diskussion. Dr. Sebastian Sprenger informierte über Entstehung und Zielsetzung der DATEV Stiftung Zukunft, die auch die Initiative „Datenschutz geht zu Schule“ fördert und auch diesen Dozententag ermöglichte. Für die DATEV-Stiftung Zukunft steht der Mensch im Mittelpunkt – die Digitalisierung muss ihm dienen. So fördert sie neben Projekten im Finanz-, des Rechts-, Steuer- und Genossenschaftswesens auch weitere Sensibilisierungseinrichtungen.

Einen Überblick über aktuelle Entwicklungen in der Gesetzgebung, der Rechtsprechung und Verlautbarungen seitens der Aufsichtsbehörden vermittelte ich im Anschluss. Nach der Mittagspause wurde die Gelegenheit genutzt, sich bei einer Führung durch das Heinz-Nixdorf-Forum die Geschichte der Datenverarbeitung in den vergangenen 200 Jahren von der Hollerith-Maschine mit der Erfindung der Lochkarte über die standardisierte Datenerfassung und Auswertung bis hin zum Einfluss von künstlicher Intelligenz auf das menschliche Zusammenleben bewusst zu machen. Danach stellten für die Verbraucherzentrale Bayern e.V. Marlene Söllner und Juliane von Behren das Angebot zu den Betroffenenrechten vor und welche Vermittlungsmöglichkeiten die Verbraucherzentralen zu den digitalen Fragen anbieten.

BvD-Vorstandsvorsitzender Thomas Spaeing bot zum Schluss einen Rückblick der DSgzS-Entstehungsgeschichte und einen Ausblick auf die Vorhaben 2020. In diesem Jahr beteiligte sich erstmals der Weka-Verlag mit der Zeitschrift Datenschutz-PRAXIS am Dozententag, ermöglichte damit den Aktionstag und produzierte dazu noch einen Podcast zur Initiative.

Hören Sie den Podcast zu „DSgzS“ der Website „Datenschutz-Praxis“. Über den QR-Code gelangen Sie direkt dorthin.

Auch 2020 ist wieder ein Dozententag geplant. Die Dozenten werden frühzeitig informiert, damit sie den Termin in ihrer Planung berücksichtigen können. Aber auch das kann nur ein kleines Zeichen der Anerkennung für den ehrenamtlichen Einsatz sein, um Schülerinnen und Schüler frühzeitig zum verantwortungsvollen Umgang mit eigenen und fremden Daten zu sensibilisieren.

Anzeige

DSGVO Praxis-workshops für Datenschutz-beauftragte.

Jetzt exklusive Praxis-Tipps sichern!

Seit Mai letzten Jahres ist die Anwendung der EU-DSGVO Pflicht. Dennoch gibt es in vielen Unternehmen noch große Unsicherheiten. Vor allem jetzt – wo die ersten schweren Strafen verhängt worden sind.

Sie kämpfen in Ihrem Arbeitsalltag auch noch mit der Umsetzung?
Wir bieten Ihnen einen Praxisworkshop, in dem es nur um praxisrelevante Inhalte und Fragen geht!

Ihre Vorteile im Überblick:

- Praktische Beispiele und Übungen stehen im Vordergrund und helfen Ihnen bei der Umsetzung der DSGVO.
- Sie können in den Erfahrungsaustausch mit anderen Teilnehmern und dem Dozenten gehen und Ihre ganz konkreten individuellen Fragen und Probleme klären.
- Durch reale Fallbeispiele arbeiten Sie datenschutzrelevante Themen durch und auf.
- Wir stellen Ihnen Vorlagen, Praxistipps und Handlungsempfehlungen zur Verfügung.

Weitere Infos und alle Termine finden Sie unter www.tuv.com/seminar-32118

Wir freuen uns auf Ihre Teilnahme!

PS: Unser gesamtes Datenschutzportfolio, inklusive aller Lehrgänge, neuer Seminare und Event-Ankündigungen finden Sie unter www.tuv.com/datenschutz

Sollten Sie vorab noch Fragen haben, stehen wir Ihnen gerne zur Verfügung.

Sandra Fahling
Business Managerin Datenschutz
Tel. 0221 – 806 3561
sandra.fahling@de.tuv.com

www.akademie.tuv.com

TÜVRheinland®
Genau. Richtig.

DATEN- UND PERSÖNLICHKEITSSCHUTZ IM ARBEITSVERHÄLTNIS

Stephan Weth, Maximilian Herberger, Michael Wächter, Christoph Sorge

Das Praxishandbuch gibt in seiner Neuauflage einen systematischen Überblick über das sensible Thema des Beschäftigtendatenschutzes. Unter Berücksichtigung der aktuellen Rechtslage und vor dem Hintergrund der DSGVO und des BDSG werden offene Fragen beantwortet und Lösungswege für Zweifelsfälle aufgezeigt. In einem eigenen Teil werden Spezialfragen zu Betriebsrat, internationalem Datentransfer, Konzerndatenschutz, Outsourcing von Dienstleistungen sowie strafrechtliche Folgen geklärt.

Im Vergleich zur 1. Auflage wurde die 2. Auflage um das Thema „Privacy by Default" und „Privacy by Design" sowie um das Thema des Arbeitnehmerdatenschutzes bei Unternehmenstransaktionen ergänzt. Des Weiteren wurde in die neue Auflage der Teil D „Praxisteil" mit Handlungsempfehlungen unter anderem zu Verarbeitungen im Konzern und zur Datenportabilität aufgenommen sowie um Hinweise und Muster für Betriebsvereinbarungen erweitert.

In einem allgemeinen Teil (Teil A) und einem besonderen Teil (Teil B) werden Aspekte des Schutzes der Arbeitnehmerdaten, von traditionellen Datenbanken bis hin zu sozialen Netzwerken beleuchtet und jeweils Vorschläge zur Lösung von Zweifelsfällen angeboten. Ein eigener Teil ist Spezialfragen (Teil C) gewidmet, wie Betriebsrat und Datenschutz, internationaler Datentransfer, Datenschutz im Konzern, Outsourcing von Dienstleistungen sowie strafrechtliche Folgen.

Das Handbuch beleuchtet „die automatisierte Einzelentscheidung", „die Befugnis zur Personalaktenführung" und „elektronische Personalakte", gibt Hinweise zur Verwendung von gesundheitsbezogenen Daten und ihren Quellen sowie zur Rechtmäßigkeit biometrischer Verfahren, verbunden mit den Rechten und Anforderungen des Betriebsrats.

Stephan Weth, Maximilian Herberger, Michael Wächter, Christoph Sorge
»Daten- und Persönlichkeitsschutz im Arbeitsverhältnis«
Praxishandbuch zum Arbeitnehmerdatenschutz

Verlag C.H. Beck

2. überarbeitete Auflage, München 2019
769 Seiten
109,00 Euro
ISBN 978-3-406-71186-2

Gerade vor dem Hintergrund der DSGVO und des BDSG gibt dieses Handbuch einen sehr guten Überblick über die ungeregelten Problemkreise und bietet Lösungshinweise und -ansätze. Es enthält umfassende Darstellungen von Anforderungen aus der Praxis und bietet hilfreiche Muster.

Empfehlenswert ist auch Kapitel 1 des Allgemeinen Teils (Teil A). Ein Durchlesen und ein in Erinnerungrufen des Arbeitnehmerdatenschutzsrechts – im Rückblick, wie alles begann, der Kampf um das Beschäftigtendatenschutzrecht, der Einfluss des EU-Rechts – ist hilfreich für das allgemeine Verständnis.

Wer das Praxishandbuch von vorn bis hinten durchliest – was aber nicht erforderlich ist – wird auf fast jede Frage zum Beschäftigtendatenschutz vorbereitet sein und zumindest einen Lösungsansatz finden. Die Gliederung mit einem umfassenden Stichwortverzeichnis erleichtert das Finden von Themen und liefert Argumente für eine Entscheidungsfindung

Fazit:

Das Praxishandbuch beleuchtet und beschreibt umfassend und systematisch die Herausforderungen im Bereich Arbeitnehmerdatenschutz. Es bietet Lösungsansätze und Arbeitshilfen für einen sicheren Umgang mit Arbeitnehmerdaten. Es ist speziell für erfahrene Praktiker im Datenschutz, die für komplexe Fragestellungen im (internationalen) Beschäftigtendatenschutz Informationen und Hintergründe benötigen. Ein gelungenes und sehr empfehlenswertes Nachschlagewerk.

DSGVO-KOMPENDIUM

Dr. Jens Eckhardt, Rudi Kramer, Sebastian Tausch

Das Kompendium ist unterteilt in zehn Kapitel:

I. Die DSGVO: Einführung
II. Grundprinzipien der DSGVO
III. DSGVO: Interne Organisation des Datenschutzes
IV. Anforderungen an die Rechtmäßigkeit
V. Erweiterte Aufgaben durch die DSGVO
VI. Schnelle erste Schritte zur Umsetzung der DSGVO
VII. Schwerpunkte der Datenschutz-Neuausrichtung
VIII. Transparenzvorgaben der DSGVO
IX. ePrivacy
X. DSGVO, BDSG und DS-AnpUG

Das Buch wird durch zahlreiche Praxis-Tipps, „Aber Achtung"-Hinweise und Anwendungshinweise abgerundet. Für Einsteiger hilfreich ist die Mustervorlage zur Anwendungserfassung in Kapitel VI. Entgegen den gängigen Templates beschränkt es sich nicht nur auf Fragen, welche mit Ja/Nein zu beantworten sind, sondern ist ergänzt um daraus gegebenenfalls resultierende To-dos, Anmerkungen und Zusatzfragen.

Im V. Kapitel wird die Auftragsverarbeitung thematisiert: Neugestaltung von Verträgen, Subunternehmerprüfung, Joint Controller und deren Abgrenzung sowie Hinweise zu weiteren Regelungen im Kontext der Auftragsverarbeitung. „Erste schnelle Schritte zur Umsetzung der DSGVO" (VI. Kapitel) enthält eine entsprechende Checkliste und beschreibt außerdem fünf wesentliche Schritte zur Umsetzung der DSGVO. Beides ist auch für den Praktiker „zum Abhaken" hilfreich.

Das Nachschlagewerk erscheint auf den ersten Blick etwas ungewohnt. Es „hangelt" sich nicht wie andere Lehrbücher durch die Artikel des Gesetzes, sondern erläutert Schritt für Schritt und schlüssig. Es ist gut durchdacht und praxisbezogen aufgebaut. Auf ein Zitieren von Artikeln wurde weitestgehend verzichtet. Einen aktuellen Gesetzestext wie auch eine englische Textfassung sollte man sowieso parat haben. Stattdessen wird der Inhalt der Regelungen erläutert und um Praxishinweise ergänzt.

Fazit:

Das Kompendium ist für Einsteiger und (erfahrene) Praktiker gleichermaßen geeignet. Es gibt hilfreiche und strukturierte Erklärungen und Hinweise. Nicht nur zum Gesetzestext, sondern besonders für die Praxis. Ein Stichwortverzeichnis wäre hilfreich. Die praxiserprobten Autoren haben eine gute Balance von Theorie und Praxis, Tipps und Wissen gefunden. Ein rundum gut gelungenes Handbuch.

Dr. Jens Eckhardt, Rudi Kramer, Sebastian Tausch
»DSGVO-Kompendium«

TKMmedia, ein Unternehmensbereich der VNR Verlag für die Deutsche Wirtschaft AG

Bonn 2019
111 Seiten
129,95 Euro
ISBN-13: 978-3812525800

Rezensionen von
Regina Mühlich
Geschäftsführerin der AdOrga Solutions GmbH, www.AdOrgaSolutions.de, Datenschutzbeauftragte, Datenschutz-Auditorin, Compliance Officer, anerk. Sachverständige für Informationsverarbeitung und Datenschutz, zert. Informationssicherheitsbeauftragte ISO/IEC 27001 (ISMS), Vorstandsmitglied des BvD e.V.

MEIN RECHT AUF DATENSCHUTZ NACH DER DATENSCHUTZ-GRUNDVERORDNUNG

Thomas Kranig, Eugen Ehmann

Das Autorenteam hatte schon mit der in der gleichen Edition herausgegebenen Information „Erste Hilfe zur Datenschutzgrundverordnung" einen kleinen Bestseller geschaffen und muss allein deshalb in der BvD-News nicht weiter vorgestellt werden.

Mit der Ergänzung durch die vorliegende Broschüre richten sie sich an die betroffenen Personen, die durch die DS-GVO adressiert werden. Ausgehend von Art. 8 der Europäischen Grundrechtecharta und vor dem Hintergrund zunehmender Digitalisierung von Dienstleistungen und dem Einsatz von Big-Data-Szenarien sowie Künstlicher Intelligenz stellen die Autoren die Spielregeln dar, wie betroffene Personen ihre Kontrollrechte wahrnehmen können. Dabei möchten sie explizit nicht diejenigen adressieren, für die das Datenschutzrecht nur eine andere Ebene anderweitig bestehender Konflikte bietet, sondern nur diejenigen, die eine echte Sorge um den zulässigen Umgang mit den eigenen personenbezogenen Daten umtreibt.

Durch Beispiele und Muster soll die Broschüre aber auch für Verantwortliche Orientierung und Maßstab bieten, was betroffene Personen als Reaktion beziehungsweise organisatorische Vorbereitung bei Unternehmen und Behörden erwarten können. Komplettiert werden die Darstellungen durch die Einbeziehung der Sichtweise der Verbraucherzentrale Bayern, die zunehmend durch betroffene Personen als Interessenswahrer eingebunden wird.

Die Broschüre gliedert sich in acht Kapitel und wird in einem Anhang mit Definitionen, Verweis auf Muster auf der Homepage des BayLDA und einer Linkliste ergänzt. Ausgehend von einer kurzen Einführung mit Erläuterung der wesentlichen Definitionen und einer Übersicht über die Rechte und Ansprechpartner werden im dritten Kapitel die einzelnen Rechte der betroffenen Person beschrieben.

Thomas Kranig, Eugen Ehmann
»Mein Recht auf Datenschutz nach der Datenschutz-Grundverordnung«

Verlag C.H. Beck München

1. Auflage 2019
56 Seiten
5,90 Euro
ISBN-13: 978-3406728754

Es folgt die Darstellung weiterer Ansprechpartner wie Datenschutzbeauftragter und Aufsichtsbehörden mit deren jeweiligen Aufgaben, Befugnissen und Kompetenzen. Den Ausführungen der Rechtsbehelfe sowie den Möglichkeiten, eine Verbraucherschutzeinrichtung einzuschalten, folgt abschließend die Abgrenzung, welche Rechte explizit nicht bestehen.

Innerhalb der einzelnen Kapitel finden sich neben Beispielen und Tipps auch Musterformulierungen. Die Sprache richtet sich ausschließlich an den interessierten Laien, Fachbegriffe werden so erläutert, dass Laien damit umgehen können.

Insbesondere das Kapitel zur Klarstellung, welche Rechte nicht bestehen, hilft, falsche Vorstellungen mit einer zitierfähigen Quelle zu widerlegen, die durch qualitative unzureichende Darstellungen durch manche Verbände und Medien gefördert wurden. Dazu gehören auch, Datenverarbeitung dürfe nur noch auf Basis einer Einwilligung erfolgen oder es bestünde ein grundsätzliches Recht, jeder Verarbeitung zu widersprechen.

Die Broschüre ist sehr empfehlenswert, auch wenn gelegentlich Aussagen in ihrer Allgemeinheit zur Diskussion einladen. Doch sie vermittelt einem Verantwortlichen und seinen Beratern die Aspekte der Rechte der betroffenen Person aus deren Perspektive und bietet – bei allen Unsicherheiten, die weiterhin in der Auslegung der europarechtlichen Normen noch bestehen – eine Zitierfähigkeit, die auch gegenüber kritischen Mitbürgerinnen und Mitbürgern hilfreich sein kann.

COMPLIANCE-NACHWEIS ZUM WEB-TRACKING NACH DSGVO

Kristin Benedikt, Alexander Buckel, Jan-Hendrik Mammen

Kristin Benedikt, Alexander Buckel,
Jan-Hendrik Mammen
»Compliance-Nachweis zum Web-Tracking nach DSGVO«

Verlag: Independently Published

78 Seiten
14,95 Euro
ISBN-13: 978-1079498424

Das Autorenteam hat sich längst einen Namen gemacht mit zwei vorher erschienen Broschüren zum „Web-Tracking nach DSGVO" und „DSGVO und ePrivacy-VO auf Webseiten umsetzen". Nun brachte es eine dritte Broschüre heraus, die sich mit den Nachweispflichten beim Webtracking unter Compliance-Gesichtspunkten zur Einhaltung der DSGVO befasst.

Die Autoren richten sich mit dem Werk an die Webseitenverantwortlichen in Unternehmen, Vereine, an Freiberufler aber auch an Blogger, um diese mit praktischen Hinweise vor einem Bußgeldrisiko beim regelwidrigen Einsatz von Webtracking-Maßnahmen zu bewahren. In der Praxis der Aufsichtsbehörden hat sich gezeigt, dass die Kontrolle der Einhaltung der rechtlichen Vorgaben der ausreichenden Information und des Einsatzes von weiteren Tools und Cookies durch fast jedermann möglich ist, so dass es nicht verwundert, wenn ein Großteil der Beschwerden, die bei Aufsichtsbehörden eingereicht werden, diese Thematik betrifft.

Auch wenn alle drei Autoren bei einer Aufsichtsbehörde beschäftigt sind und betonen, dass die Veröffentlichung keine offizielle Aussage ihres Arbeitgebers darstellt, kann davon ausgegangen werden, dass die beschriebenen Anforderungen auch gegenüber Datenschutzaufsichtsbehörden als vertretbar gelten dürften.

Den jeweiligen Checklisten und Erfassungsblättern werden unmittelbar Erläuterungen zu den auszufüllenden Feldern gegenübergestellt. Dies erleichtert das Ausfüllen.

So wird man durch die abgefragten Angaben zum Verantwortlichen und zum eingesetzten Tool geführt. Die Felder erfüllen zugleich die Anforderungen, die man für das Verzeichnis der Verarbeitungstätigkeiten benötigt.

Zum einen überrascht die Detailtiefe der einzelnen Checklisten und Dokumentationsbögen. Andererseits hilft es einem, mögliche aus Datenschutzsicht aufkommende Fragen gezielt beantworten zu können und die Informationen in das Verzeichnis nach Art. 30 DSGVO zu überführen. Die Erläuterungen erklären dem datenschutzrechtlichen Laien die Anforderungen an die Informationspflichten und die Anforderungen bei Datenschutzverletzungen, einschließlich der Betroffenenrechte. Die Broschüre selbst beinhaltet Dokumentationsmöglichkeiten von insgesamt drei Trackingtools. Sie bietet aber nicht nur für Laien ein handhabbares Instrument, datenschutzrechtliche Anforderungen bei dem Einsatz von Tracking-Tools auf Webseiten zu erkennen und deren Umsetzung zu dokumentieren.

DATENSCHUTZ-COMPLIANCE NACH DER DSGVO

Thomas Kranig, Andreas Sachs, Markus Gierschmann

Bereits die Erstauflage war eine Bereicherung. Das Autorenteam besteht unverändert aus dem Präsidenten des Bayerischen Landesamtes für Datenschutzaufsicht (BayLDA), dem Leiter des Referats Technischer Datenschutz und IT-Sicherheit des BayLDA und einem auf Datenschutzmanagement spezialisiertem Unternehmensberater. Ihre bisherige Betrachtungsweise auf die DSGVO aus dem Blickwinkel eines Juristen, Informatikers und Wirtschaftsingenieurs behalten sie bei, um sich mit der Frage auseinanderzusetzen, was aus Compliance-Sicht bei der DSGVO zu beachten ist.

Wie die Autoren in ihrem Vorwort anmerken, sehen sie weiterhin Unterstützungsbedarf bei Verantwortlichen insbesondere hinsichtlich der Umsetzung der Anforderungen der Rechenschaftspflicht. Mit dem vorliegenden Werk möchten sie dazu eine Hilfestellung geben, die eine systematische Herangehensweise an die Datenverarbeitung, die Sicherstellung der Betroffenenrechte und die Handhabung von Datenschutzverletzungen unterstützt.

Explizite Zielgruppe des Werkes sind weiterhin die Verantwortlichen, die über Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheiden. Auftragsverarbeiter sind nicht konkret adressiert, die Ausführungen zur Auftragsverarbeitung wurden jedoch erheblich erweitert. Ebenso wurden die Ausführungen zu Art. 25 DSGVO breiter dargestellt.

Das Werk umfasst unverändert drei Teile, Einführung in die DSGVO, Sicherstellung der Datenschutz-Compliance und Überwachung der Datenschutz-Compliance. Im ersten Teil werden die wesentlichen Datenschutzprozesse der datenschutzkonformen Datenverarbeitung, der Sicherstellung der Betroffenenrechte und die Handhabung von Datenschutzverletzungen als Teil der Ablauforganisation dargestellt. Die Aufbauorganisation mit den Datenschutzstrukturen über Datenschutzziele, Datenschutz-Governance-Strukturen sowie der Datenschutzleitlinie bildet den weiteren Schwerpunkt des übersichtsartigen ersten Teils.

Im zweiten Teil finden sich dann detaillierte Ausführungen zu den Datenschutzprozessen der Ablauforganisation wieder. Unterstützt von vielen grafischen Abbildungen werden anschaulich die Organisationabläufe der einzelnen rechtlichen Anforderungen erläutert. Neben dem Datenschutz-Risikomanagement umfasst dies die Datenschutzdokumentation, die Sensibilisierung zum Datenschutz, die Thematik des Datenschutzaudits beziehungsweise der Datenschutzzertifizierung sowie das Datenschutz-Managementsystem. Ein dabei immer wieder eingeforderter Prozessschritt ist der PDCA-Zyklus, Plan-Do-Check-Act, der in vielen Organisationsstrukturen bereits bei der Informationssicherheit implementiert ist.

Die Ausführungen zum Risikomanagement beinhalten eine detaillierte Darstellung der Anforderungen an einen risikobasierten Ansatz und an einen Risikomanagementprozess. Die Matrix zur Risikobewertung folgt den Festlegungen in der ISO 29134 und wird durch anschauliche grafische Abbildungen gut nachvollziehbar vermittelt. Hinsichtlich der Umsetzung einer Datenschutz-Folgenabschätzung werden die Schritte zur Risikoidentifikation, der Risikoanalyse und der Risikoevaluation erläutert, bevor dann die Ausführungen zu den Risikobehandlungsoptionen folgen. Auch den in der DSGVO gestiegenen Dokumentations- und Nachweispflichten (vgl. Art. 5 Abs. 2) wird durch eine tabellarische Aufliste der Dokumentationsanforderungen und grafischen Darstellungen Rechnung getragen, die auch die implizierten Dokumentationen beschreibt.

Im abschließenden dritten Teil werden die Befugnisse der Aufsichtsbehörden dargelegt, bevor mehreren Prüffragen zu den einzelnen Maßnahmen eine Selbstprüfung ermöglichen. Am Ende werden noch die insgesamt 94 Abbildungen und die 29 Tabellen aufgelistet und geben eine schnelle Übersicht zu den einzelnen Themen.

Das Buch ist nach wie vor uneingeschränkt empfehlenswert. In überschaubarem Umfang fasst es die wichtigsten prozessualen Anforderungen an die Umsetzung der DSGVO zusammen. Die vielen grafischen Darstellungen erleichtern es, die Komplexität der Zusammenhänge zu erfassen. Es ist eine verlässliche Unterstützung nicht nur für denjenigen, der als Verantwortlicher die Vorgaben zu beachten hat, sondern auch für dessen datenschutzrechtlichen Berater.

Thomas Kranig, Andreas Sachs, Markus Gierschmann
»Datenschutz-Compliance nach der DSGVO«

Reguvis - Bundesanzeiger Verlag

2. Auflage 2019
280 Seiten
46,00 Euro
ISBN-13: 978-38462 10239

HANDBUCH IT- UND DATENSCHUTZRECHT

Astrid Auer-Reinsdorff, Isabell Conrad et. al.

Das sehr umfassende Werk hat sich zum Ziel genommen, die Grundlagen für die Erlangung des Fachkundenachweises zur Fachanwaltsbezeichnung IT-Recht zu vermitteln. Dementsprechend umfassend wurde es. Die über 50 Autoren, die hier zusammengeführt wurden, sind ausgewählte Experten. Die Praxisnähe des Handbuchs wird allein schon durch die Zusammenarbeit mit „davit", der Arbeitsgemeinschaft IT-Recht im deutschen Anwaltsverein, sichergestellt. Dementsprechend behandelt das Werk die Anforderung an die nachzuweisenden besonderen Kenntnisse im Informationstechnologierecht gemäß § 14 k Fachanwaltsordnung (FAO). Aber das Handbuch geht noch weit darüber hinaus.

Es gliedert sich in neun Teile, die von A bis I strukturiert und in insgesamt 46 Kapitel unterteilt sind. Besonders gut gefällt mir dabei, dass in Teil A mit der Einführung in die technischen und organisatorischen Grundlagen begonnen wird, ein Themengebiet, welches § 14 k FAO nicht explizit aufführt, aber dessen Kenntnis und Verständnis in der Praxis elementar ist, um eine rechtliche Bewertung im IT-Umfeld auf belastbare Füße zu stellen.

In den weiteren Teilen werden mit Immaterialgüterecht, Software-, Hardware- und Providerverträge, der Vertrieb und elektronische Geschäftsverkehr, Telekommunikationsrecht, Datenschutz, Sicherheit und Insolvenz, Compliance und Sicherheitsrecht, Kartellrecht und Vergaberecht, Haftungsrecht und Strafrecht sowie Verfahrens- und Prozessrecht die Anforderungen des § 14k FAO dargestellt.

Dem Datenschutzrecht widmet der Band allein über 500 Seiten, wobei auch an anderen Stellen, beispielsweise beim Online-Marketing, den Ausführungen zu Apps und Social Media oder zur elektronischen Kommunikation die datenschutzrechtlichen Aspekte nicht ausgespart, sondern ausführlich erläutert werden.

Die datenschutzrechtlichen Themen behandeln die Herausgeber explizit in den Kapiteln 33 bis 36: Angefangen von den Complianceanforderungen bei der Datenverarbeitung, über das Recht des Datenschutzes und die grenzüberschreitende Datenverarbeitung bis hin zu Datenschutz im Internet.

Positiv hervorzuheben sind Darstellungen wie etwa bei der Übersichtstabelle zu den Angaben im Verzeichnis der Verarbeitungstätigkeiten des Verantwortlichen im

Astrid Auer-Reinsdorff, Isabell Conrad et. al.
»Handbuch IT- und Datenschutzrecht«

Verlag C.H. Beck

3. Auflage 2019
2.945 Seiten
349,00 Euro
ISBN-13: 978-3406721779

Vergleich zu Art. 13-15 DSGVO, die einen schnellen Überblick der Zusammenhänge ermöglichen. Ebenso fällt positiv auf, dass immer wieder Beispiele, Formulierungsvorschläge und Checklisten angeboten werden, um komplexe Darstellungen anschaulich zu machen, auf bereits ergangene Entscheidungen zu verweisen, das ausgeführte Themengebiet in die Praxis umzusetzen oder auch nur im konkreten Fall abzuprüfen. Die Datenschutz-Folgenabschätzung wird anhand des Standarddatenschutzmodells ausführlich aufgezeigt. Hier hätte man gerade für Verantwortliche im internationalen Umfeld auch einen erweiterten Verweis auf die ISO/IEC 29134 erwarten können.

Gleichwohl überzeugt das umfassende Werk durch seine Detailtiefe ohne unübersichtlich zu werden. Es eignet sich auch für Datenschutzbeauftragte, die die weiteren Zusammenhänge einer komplexen Fragestellungen nachvollziehen wollen. Es ist darüber hinaus für jeden zu empfehlen, der sich einen umfassenden Über- und Einblick in die aktuelle Rechtslage verschaffen möchte.

Auch wenn der Fachanwalt IT-Recht nicht angestrebt wird, bietet sich dieses Handbuch als hilfreicher Begleiter durch ein komplexes Rechtsgebiet an, und das nicht nur für größere Einrichtungen mit umfassenden Fragestellungen. Aufgrund der zunehmenden Digitalisierung und der angestrebten digitalen Transformation von alltäglichen Geschäftsprozessen betreffen die behandelten Themen jedes Unternehmen – gleich welcher Größe. Die Investition in dieses Handbuch rechtfertigt sich daher allein schon aus diesem Grund.

WEB-TRACKING NACH DSGVO

Kristin Benedikt, Alexander Buckel, Jan-Hendrik Mammen

Kristin Benedikt, Alexander Buckel, Jan-Hendrik Mammen
»Web-Tracking nach DSGVO«

Verlag: Independently Published

1. Auflage 2019
125 Seiten
14,95 Euro
ISBN-13: 978-1079498424

Das Autorenteam ist bereits aus einer anderen Publikation zur rechtskonformen Webseitengestaltung bekannt („DSGVO und ePrivacy-VO auf Websites umsetzen"). Alle drei Autoren sind beim Bayerischen Landesamt für Datenschutzaufsicht beschäftigt und in ihren jeweiligen Aufgabenbereichen mit technischen Analysen und rechtlichen Bewertungen betraut. Die dadurch gewonnene Expertise findet sich in dieser Broschüre wieder. Auch wenn es sich nicht um eine offizielle Broschüre einer Aufsichtsbehörde handelt, kann davon ausgegangen werden, dass sämtliche Aussagen eine rechtskonforme Umsetzung der datenschutzrechtlichen Anforderungen im Sinne der Datenschutzaufsichtsbehörden sicherstellen.

Wie bei ihrem (o.g.) ersten gemeinsamen Werk begleiten Sie einen fiktiven „Webmaster Mike" bei seiner Tätigkeit und den damit verbundenen Fragestellungen rund um das Thema „Tracking". In vier Kapiteln werden insgesamt 78 Fragen verteilt, die sich nicht auf die Beantwortung mit juristischen Hinweisen begnügen, sondern zusätzlich mit Grafiken und weiterführenden Links konkrete Umsetzungshilfen anbieten. So werden in den ersten drei Kapiteln Ausführungen zur Rolle des Datenschutzes, zu den jeweiligen Rechtsgrundlagen und Informationspflichten erörtert, bevor im 4. Kapitel weitere rechtliche Rahmenbedingungen wie der Umgang mit den Rechten der betroffenen Person beschrieben werden.

Für die praktische Umsetzung sehr hilfreich sind die anschließenden Muster zu Consent-Banner, ein Überblick zu Tracking-Tools im Quick-Check sowie eine kurze Darstellung der Compliance-Nachweise für Webseiten-Betreiber.

Da der EuGH in seiner „Planet49"-Entscheidung vom 1. Oktober 2019 (Az C-673/17) keine weiteren Anforderungen an den Einsatz von technischen Möglichkeiten auf Webseiten (wie etwa Cookies) bei der Verarbeitung personenbezogener Daten zu Werbezwecken stellte – wie bisher die Datenschutzkonferenz – können die Aussagen, Hinweise und Muster in dieser Broschüre auch nach der EuGH-Entscheidung verwendet werden.

Die Broschüre ist für alle sehr empfehlenswert, die Webseiten gestalten oder zu deren rechtlichen Anforderungen beratend unterstützen. Sie veranschaulicht in einer klaren Sprache die Anforderungen und gibt praxisnahe Tipps zur Umsetzung.

Rezensionen von

Rudi Kramer
ist Rechtsanwalt und Sprecher des AK Schule im BvD. e.V."

HANDBUCH BESCHÄFTIGTENDATENSCHUTZ - AKTUELLE RECHTSLAGE UND UMSETZUNGSHILFEN

Prof. Dr. Peter Gola

Prof. Dr. Peter Gola
»Handbuch Beschäftigtendatenschutz - aktuelle Rechtslage und Umsetzungshilfen«

Verlag DATAKONTEXT GmbH

8. komplett neu bearbeitete Auflage 2019
726 Seiten
Preis: 139,99 €
ISBN-13: 978-3-89577-801-8

Das Standardwerk zum Thema - nun in aktueller Auflage. Mit der neuen Auflage hat nicht nur der Titel von Arbeitnehmerdatenschutz in Beschäftigtendatenschutz gewechselt, sondern den Neuerungen durch die DSGVO und das neue BDSG wurde durch eine Änderung der Konzeption des Werkes Rechnung getragen.

Nicht geändert hat sich die bewährte Qualität und Praxisnähe der Darstellung. Die neue Rechtslage wird umfassend dargestellt und anhand zahlreicher Fallbeispiele und unter Bezugnahme auf die Rechtsprechung erläutert. Wenngleich es zur neuen Rechtslage natürlich noch kaum Rechtsprechung gibt, muss gesehen werden, dass es erhebliche Parallelen zwischen dem § 32 BDSG-alt und § 26 BDSG sowie der alten und neuen Rechtslage im Beschäftigtendatenschutz gibt. Die seit der Vorauflage erschienene Literatur sowie die Arbeitshilfen und Hinweise der Aufsichtsbehörden zur Umsetzung der DSGVO und dem BDSG werden ebenfalls berücksichtigt. Hiervon ausgehend werden gerade auch für Zweifelsfälle und offene Fragestellungen Lösungen in der Praxis angesprochen.

Das Werk ist in 20 Kapitel mit einer Mehrzahl an Unterkapiteln gegliedert. Diese Aufteilung berücksichtigt direkt erkennbar und damit gut strukturiert die Änderungen der Rechtslage. So wird in einzelnen Kapiteln die automatisierte Einzelentscheidung (Art. 22 DSGVO), die einzelnen Verarbeitungszwecke des § 26 Abs. 1 Satz 1 BDSG, die Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO, § 26 Abs. 3 BDSG) und die Kollektivvereinbarung (§ 26 Abs. 4 BDSG) behandelt. Abgeschlossen wird das Buch durch eine Übersicht höchstrichterlicher Rechtsprechungen in Leitsätzen und ein umfassendes Literaturverzeichnis.

Das Werk umfasst zudem den Online-Service für digitale Inhalte des Werks (E-Book zum Download). Jedes Werk enthält einen Code für eine einmalige Registrierung.

Das Buch richtet sich an Juristen, Betriebsräte, Personalverantwortliche, Datenschutzbeauftragte, Datenschutzverantwortliche, Compliance-Beauftragte und Führungskräfte.

Es wird seinem Anspruch gerecht, diesen eine sowohl inhaltlich qualifizierte als auch praxisnahe Aufarbeitung des Beschäftigtendatenschutzes zu liefern. Das Werk ist zu empfehlen!

Rezension von

Dr. Jens Eckhardt
Rechtsanwalt
Fachanwalt für Informationstechnologierecht
Datenschutz-Auditor (TÜV)
Compliance Officer (TÜV)
Vorstandsmitglied des BvD e.V.

TERMINE DER REGIONALGRUPPEN UND ARBEITSKREISE DES BVD

Die wichtigsten Daten der BvD-Gremien

Die Arbeitskreise und Regionalgruppen sind wichtige Gremien innerhalb des BvD. Detaillierte Informationen zu den Treffen und den Terminen finden Sie unter:

▶ www.bvdnet.de/regionalgruppen **bzw.**

▶ www.bvdnet.de/arbeitskreise

Die nächsten Treffen unserer Arbeitskreise und Regionalgruppen:

17.01.2020	AK EVU	**28.02.2020**	RG München
22.01.2020	AK Sozial	**28.02.2020**	RG Nürnberg
23.01.2020	RG Mitte	**28.02.2020**	RG Stuttgart
31.01./01.02.2020	AK Externe	**19.03.2020**	RG Ost
07.02.2020	RG Karlsruhe	**19./20.03.2020**	AK Medizin
27.02.2020	RG Langen	**23.04.2020**	AK Krypto

Sie möchten zu einem Thema aktiv mitmachen oder in Erfahrungsaustausch mit Kollegen treten?

Termine und Anmeldung finden Sie auf unserer Webseite:

▶ www.bvdnet.de

VERNETZEN SIE SICH MIT UNS:

▶ www.bvdnet.de

XING: https://www.xing.com/companies/berufsverbandderdatenschutzbeauftragtendeutschlands

TWITTER: www.twitter.com/bvd_datenschutz

BLOG: www.bvdnet.de/themen/bvd-blog/

RSS-Feed: https://www.bvdnet.de/feed/

BVD-STELLENBÖRSE

Sie suchen ausgewiesenes Datenschutz-Knowhow für Ihr Unternehmen? Mit einer Anzeige in der BvD-Stellenbörse finden

Sie zertifizierte Datenschutzbeauftragte für eine Festanstellung oder als externe Berater. Zur Stellenbörse:

▶ https://www.bvdnet.de/bvd-stellenboerse/

Anzeige

Ausblick

Seminare – 2019/2020

Termin	Thema	Ort
11.12.2019	**Social Media, Cookies, Tracking & Co. – Datenschutz und Werbung**	Düsseldorf
12.12.2019	**Datenschutzverletzungen, Prüfungen, Bußgeld**	Düsseldorf
22.01.2020	**Datenschutzverletzungen, Prüfungen, Bußgeld**	Hannover
03.02.2020	**ISO 27701**	Hamburg
11.02.2020	**IT für Datenschutzbeauftragte – Einsteigerseminar**	Frankfurt/Main
25.02.2020	**Art. 26 DSGVO – Die gemeinsame Verantwortlichkeit**	Berlin
23.03.2020	**ePrivacy-Verordnung – Praxisseminar**	Düsseldorf
03.04.2020	**Prüfen Sie Ihre Mandanten – kleines Hacking für DSB**	Nürnberg
05.05.2020	**Sonderseminar: Datenschutz durch Technik**	Berlin

* nur für BvD Mitglieder

Information und Anmeldung unter www.bvdnet.de

Anzeige

LEITZ IQ-SCHREDDER

DER PAPIERKORB 2.0 – GEH AUF NUMMER SICHER

DSGVO KONFORM*

Stephan J. aus Stuttgart,
Forschung & Entwicklung

€ 20.0 MIO SPAREN!*

*Schreddern unterstützt die Einhaltung der DSGVO. Verstöße gegen die DSGVO können mit Bußgeldern von bis zu € 20.0 Mio oder 4 % des weltweiten Jahresumsatzes des entsprechenden Unternehmens geahndet werden – je nachdem, welche Summe größer ist.

Wenn es um Datenschutz geht, ist es wichtig, keine unnötigen Risiken einzugehen. Mit einem Leitz IQ-Shredder unter Ihrem Schreibtisch sind Sie auf der sicheren Seite – denn dieser ist die intelligente Alternative zu einem Papierkorb. Er ist der Papierkorb 2.0.

Mehr unter:
www.leitz.com/shredder

LEITZ®
ALLES IM GRIFF